



CYCLED AGENCY INFORMATION SYSTEMS SECURITY REVIEW

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2019

Auditor of Public Accounts
Staci A. Henshaw, CPA

www.apa.virginia.gov

(804) 225-3350



AUDIT SUMMARY

Our audit of information systems security (ISS) at 19 agencies for the fiscal year ended June 30, 2019, had the following objectives:

- Determine whether the agency has developed adequate policies and procedures;
- Determine whether sufficient ISS controls have been implemented and are functioning as intended; and
- Determine whether the agency complies with applicable laws and regulations governing ISS controls.

We selected the 19 agencies based on multiple factors and considerations related to each agency's ISS control environment. We evaluated the same ISS controls at each agency and, for reporting purposes, categorized our work using seven general ISS control areas:

- Policies and Procedures
- Information Technology (IT) Governance
- Access Control
- Audit Logging
- Risk Management and Contingency Planning
- Security Awareness Training
- Third-Party Provider Oversight

The table below summarizes the results of our review for the 19 agencies selected, along with an assessment of the adequacy of their controls for the ISS control areas tested. Inadequate ISS control areas are detailed by agency in the “Audit Findings and Recommendations” section of the report.

Agency	Adequate ISS Control Areas
Department of Agriculture and Consumer Services	7 of 7
Department of Conservation and Recreation	2 of 7
Department of Criminal Justice Services	2 of 7
Department of Elections	3 of 7
Department of Energy	3 of 7
Department of Forestry	0 of 7
Department of Health Professions	5 of 7
Department of Housing and Community Development	5 of 7
Department of Juvenile Justice	2 of 7
Department of Labor and Industry	4 of 7
Department of Military Affairs	5 of 7
Department of Professional and Occupational Regulation	2 of 7
Department of Small Business and Supplier and Diversity	5 of 7
Indigent Defense Commission	3 of 7
Jamestown-Yorktown Foundation	2 of 7
Office of the State Inspector General	6 of 7
State Council of Higher Education for Virginia	2 of 7
Virginia Museum of Natural History	0 of 7
Virginia Workers’ Compensation Commission	7 of 7

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
INTRODUCTION	1-2
AUDIT OVERVIEW	3-5
AUDIT FINDINGS AND RECOMMENDATIONS	6-44
TRANSMITTAL LETTER	45-46
AGENCY RESPONSES	47-76
RESPONSIBLE OFFICIALS	77-78

INTRODUCTION

The Auditor of Public Accounts (APA), as required by the Code of Virginia, audits all executive and judicial branch Commonwealth agencies handling state funds. However, the Code of Virginia does not require audits of all agencies annually. The APA refers to agencies audited on a periodic basis as cycled agencies. Historically, the APA audited cycled agencies at least once every three years. Beginning with fiscal year 2016 audits, the APA developed a risk-based approach for auditing cycled agencies. This modified audit approach allows the APA flexibility to focus on different areas significant to agency operations each year based on an assessment of risk factors. For fiscal year 2019, the APA chose ISS as the area of audit focus.

Objectives

The overall objective for this audit is to gain an understanding of ISS within the cycled agency population and to identify areas of potential risk at each agency. This audit includes an analysis of the internal controls surrounding ISS, the systems used by the agency, interactions with third-party service providers, and compliance with the applicable laws and regulations governing ISS. The specific objectives of this review are to:

- Determine whether the agency has developed adequate policies and procedures.
- Determine whether sufficient ISS internal controls have been implemented and are functioning as intended.
- Determine whether the agency complies with applicable laws and regulations governing ISS controls.

Scope and Methodology

We performed our audit as of and for the fiscal year ended June 30, 2019. We included a total of 48 agencies in our risk-based analysis to determine which agencies would be included in our sample for the ISS review. We also considered the size of the agency to provide representation of both smaller and larger cycled agencies. Factors we considered included:

- whether the agency received an APA Internal Control Questionnaire (ICQ) for fiscal year 2019;
- whether the agencies received an ICQ in the prior fiscal year and whether the ICQ identified ISS issues;
- number of information systems in use;
- amount of ISS related expenses in fiscal year 2019, primarily in relation to the agency's total expenses;

- revenues as a percentage of expenses in fiscal year 2019 to gauge each agency's interaction with the public and evaluate the need to protect sensitive information; and
- prior knowledge of agencies with qualitatively significant ISS programs.

Based on our analysis of the factors above, we determined that we would perform a review of ISS at 19 agencies. Eleven of the 19 agencies included in the audit also received an APA ICQ review for fiscal year 2019. A concurrent review of the ICQ and ISS allows the APA to foster collaboration and provide a comprehensive assessment of the control environment at these 11 agencies. We selected the other eight agencies included in the audit based on risk factors, such as the number of information systems, ISS expenses, and interaction with the public. Table 1 below lists the agencies selected and provides the agencies' abbreviated names used in this report.

Agency Names and Abbreviations

Table 1

Agency	Abbreviated Name
Department of Agriculture and Consumer Services	Agriculture
Department of Conservation and Recreation	Conservation and Recreation
Department of Criminal Justice Services	Criminal Justice ¹
Department of Elections	ELECT
Department of Energy	Energy
Department of Forestry	Forestry ¹
Department of Health Professions	Health Professions ¹
Department of Housing and Community Development	Housing
Department of Juvenile Justice	Juvenile Justice ¹
Department of Labor and Industry	Labor and Industry
Department of Military Affairs	Military Affairs ¹
Department of Professional and Occupational Regulation	Professional and Occupational Regulation
Department of Small Business and Supplier Diversity	Small Business
Indigent Defense Commission	Defense Commission ¹
Jamestown-Yorktown Foundation	Jamestown-Yorktown ¹
Office of the State Inspector General	Inspector General ¹
State Council of Higher Education for Virginia	State Council ¹
Virginia Museum of Natural History	Natural History ¹
Virginia Workers' Compensation Commission	Workers' Compensation ¹

1 – These 11 agencies also received an APA ICQ during fiscal year 2019.

We used a non-statistical sampling approach and designed our samples to support conclusions about our audit objectives. By using an appropriate sampling methodology, we ensured the samples selected were representative of the population and provided sufficient, appropriate evidence. We identified specific attributes for testing each of the samples and when appropriate, we projected our results to the population.

AUDIT OVERVIEW

The Virginia Information Technologies Agency (VITA) establishes the security standards for the Commonwealth. We selected the following areas for review, as we commonly encounter issues in these areas during our audits and we consider them critical for maintaining and/or improving ISS.

- Policies and Procedures
- Information Technology (IT) Governance
- Access Control
- Audit Logging
- Risk Management and Contingency Planning
- Security Awareness Training
- Third-Party Provider Oversight

Our audit evaluated these areas against the Commonwealth of Virginia's Information Security Standard, SEC 501 (Security Standard) and the Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard). We provide an overview of each area reviewed in the following section.

Policies and Procedures

ISS policies and procedures provide the instructions to carry out an agency's ISS program. The ISS program includes the development and management of consistent, cohesive policies, processes, and decision-rights for a given area of responsibility. These policies and procedures in conjunction with the ISS program should ensure compliance with the Security Standard. We reviewed each agency's policies and procedures to determine whether they are adequate and reviewed annually.

IT Governance

IT governance is the organizational structure and processes that ensure an agency's IT supports its strategies and objectives. We audit IT governance to ensure compliance with the Security Standard and to ensure an agency has the proper IT structure in place to support its overall goals and objectives. We reviewed the structure of each agency's ISS operations including the placement, independence, and duties of the agency's Information Security Officer (ISO).

Access Control

Access controls are a set of security procedures that monitor access and either allow or prohibit users from accessing information systems. These controls protect the confidentiality, integrity, and availability of information systems. The purpose of access controls is also to prevent unauthorized access to data in information systems. We performed procedures over each agency's access control policies, annual access reviews, and access termination process.

Audit Logging

Information systems that contain sensitive information must provide authorized users with the ability to audit user activity to establish individual accountability. It is especially important to review the activities performed by accounts with elevated privileges, such as database administrator and system engineer accounts. Information systems typically include an audit logging capability, which tracks each user's access, modification, and creation of data in an information system. System credentials are unique for each user, which allows tracking of user activity and the ability to perform an independent review of all user-performed system activities. Mission-essential information systems need to provide this audit trail to ensure the adequacy of controls and compliance with laws, regulations, and internal policies. We performed procedures over each agency's audit and accountability policy and the controls that support the policy.

Risk Management and Contingency Planning

Agencies are increasingly reliant on information systems and third-party service providers, including cloud-based technologies. As these services expand, risk management practices, including the identification and implementation of information security controls, are essential to reduce risk to an acceptable level for each agency. Agencies should perform risk assessments for each information system and implement risk mitigation strategies commensurate with the agency's risk appetite.

A contingency plan allows agencies to, as quickly as possible, return to providing mission-essential functions. This plan should identify alternative strategies to be used if a disaster occurs. The recovery of an organization's information systems and data is critical to restoring operations and providing essential services to the citizenry.

It is important to note that many of the agencies reviewed in this report contract with VITA for centralized ISO services. In general, the contract engages VITA to perform and document business impact analyses, system security plans, and risk assessments for an agency's sensitive systems. However, it is still each agency's responsibility to ensure completion and review of the documentation in accordance with the Security Standard.

We reviewed each agency's information system risk assessments, business impact analyses, ISS audits, third-party service provider agreements, including with VITA's enterprise cloud oversight services (ECOS) service, and continuity of operation plans.

Security Awareness Training

Security awareness training is a key preventative control that raises employee awareness about security threats, sensitive data, incident responses, and the potential impact on the agency and the Commonwealth's interests. This type of training equips information system users with the knowledge and understanding to prevent and mitigate risks to the agency and Commonwealth. We reviewed each agency's security awareness training policy, the training topics covered, and users' training completion records.

Third-Party Provider Oversight

Agencies use third-party providers to provide services on behalf of the agencies. Software as a service is increasingly used as a means to address the constant need to reduce costs, rapidly changing technology environments, and increasing oversight requirements. In some circumstances, agencies use VITA's ECOS to provide oversight functions and management of cloud-based services. However, even when contracting with ECOS, each agency remains responsible for ensuring relevant documentation is complete and accurate in accordance with the Security Standard. We reviewed each agency's third-party provider risk assessments prior to contracting with the provider and the agency's ongoing oversight documentation.

AUDIT FINDINGS AND RECOMMENDATIONS

This report is a compilation of all findings issued to the 19 agencies. The findings are further categorized into one of seven ISS control areas to gain an overall perspective as to where agencies have deficient information security controls. Specific audit findings and their respective conclusions only apply to each individually identified agency. These conclusions cannot be extrapolated to the entire population of 48 cycled agencies nor to any other agency. Table 2 below shows the audit findings by agency and information security control area. The ✓ symbol indicates that we reviewed the control area and did not issue a finding for that agency. An X indicates that we reviewed a control area and issued findings for the specific agency. If a number accompanies the X, it signifies the number of findings issued at a particular agency for that control area, while no number indicates we issued only one finding for the control area. We did not issue any findings to Agriculture or Workers' Compensation.

Findings by Agency and Information Security Control Area

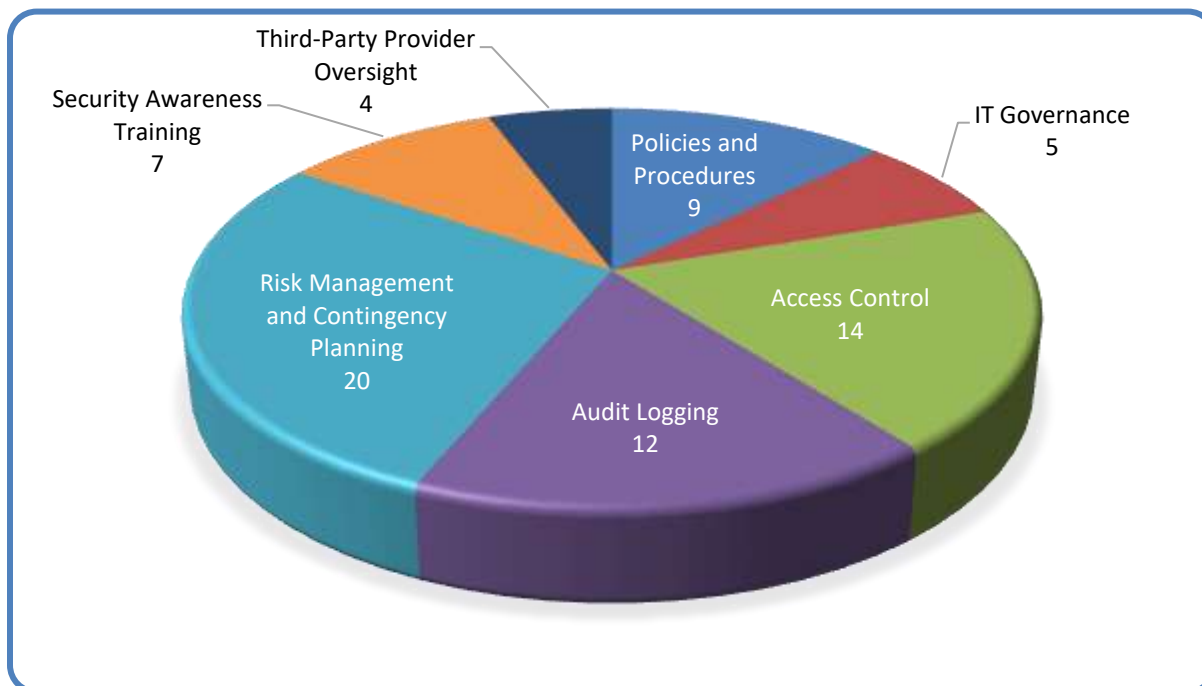
Table 2

Agency	Policies and Procedures	IT Governance	Access Control	Audit Logging	Risk Management and Contingency Planning	Security Awareness Training	Third-Party Provider Oversight
<u>Conservation and Recreation</u>	X	✓	X	X	X ²	X	✓
<u>Criminal Justice</u>	X	X	X	X	X	✓	✓
<u>Elections</u>	X	✓	X	X	X	✓	✓
<u>Energy</u>	✓	✓	X	X	X	✓	✓
<u>Forestry</u>	X	X	X	X	X	X	X ²
<u>Health Professions</u>	✓	✓	X	✓	X	✓	✓
<u>Housing</u>	✓	X	X	✓	✓	✓	✓
<u>Juvenile Justice</u>	X	✓	X	X	X ²	X	✓
<u>Labor and Industry</u>	✓	✓	X	X	X	✓	✓
<u>Military Affairs</u>	✓	✓	X	✓	X	✓	✓
<u>Professional and Occupational Regulation</u>	X	X	✓	X	X	X	✓
<u>Small Business</u>	✓	✓	✓	X	X	✓	✓
<u>Defense Commission</u>	X	✓	X	✓	X ²	✓	X
<u>Jamestown-Yorktown</u>	✓	✓	X	X	X ²	X	X
<u>Inspector General</u>	✓	✓	✓	✓	X	✓	✓
<u>State Council</u>	X	✓	X	X	X	X	✓
<u>Natural History</u>	X	X	X	X	X	X	X

Risk management and contingency planning, access control and audit logging are the control areas with the most recommendations for improvement. Generally, limited staffing resources and lack of management oversight are the main causes of the findings. Chart 1 depicts the total findings for all agencies grouped by area. As indicated in the detailed findings and recommendations below, we categorized some findings in multiple control areas. Additionally, as noted in Table 2 above, some agencies may have multiple findings within the same control area.

Findings by Control Area

Chart 1



Department of Conservation and Recreation

Review and Update Policies and Procedures

ISS Control Area: Policies and Procedures

Conservation and Recreation has not reviewed and updated its ISS policies and procedures to align with the requirements of the Security Standard since 2016. The following sections of the Security Standard require that policies and procedures be reviewed and updated on an annual basis or more frequently if required to address environmental changes: AC-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, and SI-1. In addition, Conservation and Recreation's IT Security Policy No. 427 states the ISO is responsible for "reviewing and assessing annually the Information Security policy for new or changed requirements, either internal or external, including changes in the COV or Department IT environment. This will occur in September of each year."

An annual review of policies and procedures ensures the current IT environment complies with the Security Standard. Conservation and Recreation's lack of review and updates since 2016 increases the risk of noncompliance with the Security Standard and irrelevance of existing policies and procedures to the IT environment. Noncompliance with the Security Standard may result in insufficient or inappropriate processes, increasing the vulnerability of systems and risk to the confidentiality, integrity, and availability of data.

Conservation and Recreation should develop a process to review and update all ISS policies and procedures annually or more often if changes occur in its IT environment. The process should include documentation of the update and review process.

Improve Access Controls

ISS Control Area: Access Control

Conservation and Recreation does not have adequate controls over information system access, as required by the Security Standard. Specifically, Conservation and Recreation has internal control weaknesses in the following areas:

- Conservation and Recreation does not review system access for one sensitive information system on an annual basis, as required by the Security Standard, Section AC-2.
- Conservation and Recreation does not retain documentation of the information system access review for one sensitive system, as required by the Security Standard, Section AC-2.
- Conservation and Recreation does not have documented procedures in place for information system access requests, as required by the Security Standard, Section AC-1.

- Conservation and Recreation does not disable information system access within 24-hours of employment termination, as required by the Security Standard, Section PS-4.

Inadequate access controls can result in improper or unnecessary access to sensitive systems, which can lead to a breach of data security. Conservation and Recreation does not review system access for one sensitive system as the system owner is not familiar enough with the system users to determine if granted access is appropriate. Conservation and Recreation reviews and approves system access via email and was unaware that there was a requirement to retain review documentation. Conservation and Recreation currently has access request procedures for one sensitive system; however, the procedures remain in draft form. Conservation and Recreation did not timely disable information system access due to the IT Department not being notified timely when employees separated.

Conservation and Recreation should implement a system access review process for all sensitive systems, which should include retaining documentation of the review. Conservation and Recreation should develop system access request procedures and finalize the procedures that have already been drafted. Additionally, Conservation and Recreation should develop a process to properly and timely notify all necessary individuals when an employee separates from the department.

Improve Audit Log Controls

ISS Control Area: Audit Logging

Conservation and Recreation does not implement certain audit logging and monitoring safeguards for sensitive systems in accordance with the Security Standard. We communicated two internal control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard requires audit logging and monitoring controls to protect the confidentiality, integrity, and availability of sensitive and mission-critical data. Due in part to limited personnel resources, Conservation and Recreation was not able to implement the necessary safeguards described in the FOIAE document and comply with the Security Standard.

Conservation and Recreation should dedicate the necessary resources to implement the security controls discussed in the communication marked FOIAE in accordance with the Security Standard. Implementing corrective action will help maintain the confidentiality, integrity, and availability of Conservation and Recreation's sensitive and mission-critical data.

Review and Update System Risk Assessments

ISS Control Area: Risk Management and Contingency Planning

Conservation and Recreation has not reviewed and updated its risk assessment within the last year as required by the Security Standard. The Security Standard, Section 6.2, states for each IT system classified as sensitive, the agency shall conduct and document an annual self-assessment to determine the continued validity of the risk assessment. In addition, Conservation and Recreation's IT Security

Policy No. 427 states the agency should “review risk assessment results on an annual basis or more frequently if required to address an environmental change.”

An annual review of the risk assessment for sensitive systems ensures proper consideration and reflection of the current IT environment. A lack of review and update increases the opportunity that Conservation and Recreation has not identified or properly addressed new risks or vulnerabilities. Conservation and Recreation was unaware that its risk assessment must be reviewed and updated annually as it believed that review of the risk assessment was required once every three years.

Conservation and Recreation should follow its IT Security Policy No. 427 and review and update its risk assessment on an annual basis or more frequently, if required, to address an environmental change. This review should include documentation that the review was completed.

Perform Disaster Recovery Testing

ISS Control Area: Risk Management and Contingency Planning

Conservation and Recreation is not properly testing its IT disaster recovery plan (DRP), as required by the Security Standard. Section CP-1-COV-1 of the Security Standard requires that agencies perform an annual exercise of IT disaster recovery components to assess their adequacy and effectiveness. In addition, Conservation and Recreation does not document within its DRP a strategy for testing disaster recovery procedures. Section CP-9 of the Security Standard requires all sensitive systems to have a documented strategy for testing disaster recovery procedures.

Conservation and Recreation’s normal operations include backup and restoration processes throughout the year, and the department considered this process to provide the assurance that the DRP was working as designed. Without a well-tested DRP, Conservation and Recreation may not be able to restore the systems that support mission-critical business functions promptly in the event of an emergency or disaster. Conservation and Recreation should institute and document a process for annual testing of the DRP to ensure timely restoration of mission-essential functions in the event of a disaster.

Improve Security Awareness Training Program

ISS Control Area: Security Awareness Training

Conservation and Recreation’s information system users are not completing, and monitoring security awareness training as required because the department is not enforcing compliance.

Section AT-2 of the Security Standard requires agencies to provide basic security awareness training to information system users at least annually. Additionally, Section AT-4 requires agencies to document and monitor individuals’ completion of security awareness training.

Conservation and Recreation’s current monitoring process does not ensure all employees have completed training. Information system users who do not complete security awareness training annually may lack the knowledge to identify and respond to security threats that could compromise sensitive systems and data. Conservation and Recreation should ensure information system users complete all

elements of the required security awareness training. Additionally, Conservation and Recreation should ensure the monitoring of training provides a listing of only current employees and consider disabling account access if users do not complete the required training.

Department of Criminal Justice Services

Improve IT Security Governance

ISS Control Areas: Policy and Procedures and IT Governance

Criminal Justice does not have an adequate IT security governance structure to manage its ISS program and comply with the Security Standard. The Security Standard requires agencies to ensure the ISS program is maintained, is adequate to protect the agency's IT systems, and is effectively communicated throughout the organization (Security Standard Section 2.4.2). Specifically, Criminal Justice has internal control weaknesses in the following areas:

- Criminal Justice does not have an ISO that is independent from IT operations, as required in the Security Standard, Section 2.4.1.
- Criminal Justice does not have an established, documented, implemented, and maintained ISS program that is sufficient to protect the agency's IT systems, as required in the Security Standard, Sections 1.4 and 2.4.2.
- Criminal Justice has no documented policies and procedures in place related to information security, as required in the Security Standard, Sections AC-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, and SI-1.

Criminal Justice has not allocated appropriate personnel resources to the ISS program, which has resulted in ISS responsibilities falling to those within the IT Department. The current ISO is also the senior programmer analyst and therefore, cannot provide adequate, independent oversight of IT security. By not having an adequate IT governance structure to properly manage Criminal Justice's ISS program, there is increased risk that Criminal Justice will not properly secure sensitive IT resources, which can lead to a breach of sensitive data or system unavailability.

Criminal Justice should establish an independent security function within the organization and integrate ISS with system operations. To reduce any potential conflicts of interest, the ISO should report directly to the agency head, and not to the Chief Information Officer (CIO). Criminal Justice should develop and implement policies and procedures that are compliant with the requirements of the Security Standard. Finally, Criminal Justice should evaluate its IT personnel levels to ensure sufficient resources are available to implement any IT security governance changes and remediate any internal control deficiencies. Improving the IT governance structure will help ensure the confidentiality, integrity, and availability of sensitive data.

Develop and Implement Logical Access Controls

ISS Control Area: Access Control

Criminal Justice does not have appropriate internal controls in place to ensure that access to its systems is appropriate and complies with the requirements of the Security Standard. Specifically, Criminal Justice has weaknesses in the following areas:

- Criminal Justice does not have an access control policy in operation, as required by the Security Standard, Section AC-1.
- Criminal Justice does not require a documented request from the user for access to internal IT systems and does not require confirmation of the account request including approval by the IT system user's supervisor and approval by the data owner or designee, or the ISO, to establish accounts on sensitive systems as required by the Security Standard, Section AC-2-COV.
- Criminal Justice does not have an adequate process in place for ensuring it removes access to its network and systems within 24 hours of a user's employment ending, as required by the Security Standard, Section PS-4. In a sample of three terminated employees, two of the individuals retained access to the department's network and information systems for ten and 84 days, respectively, after employment termination.
- Criminal Justice does not have an adequate process in place for reviewing and confirming ongoing operational need for current logical and physical access to information systems/facilities upon reassignment or transfer of employees to other positions within the organization, as required by the Security Standard, Section PS-5.
- Criminal Justice does not have an adequate process in place for an annual review of systems access, as required by the Security Standard, Section AC-2.
- Criminal Justice does not require system administrators to have both an administrative account and at least one user account, as required by the Security Standard, Section AC-2-COV.

Inadequate access controls can result in improper or unnecessary access to sensitive systems, which can lead to a breach in data security. Criminal Justice has not implemented an access control policy and has not allocated appropriate resources to ensuring access controls are appropriate and consistent with the requirements of the Security Standard. Criminal Justice should develop and implement access policies and procedures that align with the Security Standard to ensure consistent and appropriate account management and to ensure the protection of sensitive information.

Improve Audit Logging Capabilities and Develop a Process for Monitoring Audit Logs

ISS Control Area: Audit Logging

Criminal Justice does not implement certain audit logging and monitoring safeguards for sensitive systems in accordance with the Security Standard. We communicated three internal control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard requires audit logging and monitoring controls to protect the confidentiality, integrity, and availability of sensitive and mission-critical data. Due in part to limited personnel resources, Criminal Justice was not able to implement the necessary safeguards described in the FOIAE document and comply with the Security Standard.

Criminal Justice should dedicate the necessary resources to implement the security controls discussed in the communication marked FOIAE in accordance with the Security Standard. Implementing corrective action will help maintain the confidentiality, integrity, and availability of Criminal Justice's sensitive and mission-critical data.

Improve Disaster Recovery Plan

ISS Control Area: Risk Management and Contingency Planning

Criminal Justice has not included all the components of its DRP in its contingency planning documents and is not performing an annual exercise of the DRP components, as required by the Security Standard.

The Security Standard, Section CP-1-COV-1, requires that agencies use their business impact analysis (BIA) and risk assessments to develop IT disaster components of the agency contingency plan. These components include identification of each IT system that is necessary to recover agency business functions or dependent business functions and the recovery time objective (RTO) and recover point objective (RPO) for each. Additionally, an annual exercise of DRP components is necessary to assess their adequacy and effectiveness. Criminal Justice's continuity of operations plan includes some of the required components but does not identify the RTO and RPO for each system. Failure to include all and test necessary DRP components could result in a failure or delay when reinstituting the agency's mission-essential and primary business functions in the event of a disaster.

Criminal Justice has not allocated appropriate personnel resources to information system security, which has resulted in incomplete disaster recovery planning. Criminal Justice should revise its contingency planning documentation to ensure that all required elements of the DRP are included and should perform annual testing of the DRP components.

Department of Elections

Develop and Implement Policies and Procedures

ISS Control Area: Policies and Procedures

ELECT does not have properly executed policies and procedures documented to comply with the Security Standard. The Security Standard, Section 2.4.2, requires that an ISS program be maintained, is adequate to protect IT systems, and is effectively communicated throughout the organization. ELECT has developed draft policies; however, all necessary policies and procedures have not been approved and implemented as required in the Security Standard, Sections AC-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, and SI-1.

Limited IT personnel resources available to ELECT along with recent turnover in key ISS positions contributed to the identified weaknesses. A lack of policies and procedures surrounding ISS may result in insufficient or inappropriate processes and leaves the agency at risk for improper system usage due to lack of formal guidance. ELECT should develop, approve, and implement ISS policies and procedures to ensure that the agency's processes align with the requirements of the Security Standard.

Improve Access Controls

ISS Control Area: Access Control

ELECT does not have appropriate internal controls in place to ensure that access to its systems is appropriate and complies with the requirements of the Security Standard. Specifically, ELECT has weaknesses in the following areas:

- ELECT does not consistently require confirmation of the account request and approval by the IT system user's supervisor and the data owner or designee, or the ISO, to establish accounts on all sensitive systems, as required by the Security Standard Section AC-2-COV.
- ELECT does not have an adequate process for reviewing and confirming ongoing operational need for current logical and physical access to information systems/facilities upon reassignment or transfer of employees to other positions within the organization as required by the Security Standard, Section PS-5.
- For eight of the ten (80%) employees sampled, ELECT could not provide documentation to support the removal of systems access within 24 hours of the end of the user's employment, as required by the Security Standard, Section PS-4.
- ELECT does not have an adequate process in place for an annual review of systems access, as required by the Security Standard, Section AC-2.

Inadequate access controls can result in improper or unnecessary access to sensitive systems, which can lead to a breach in data security. Limited IT resources and personnel available to ELECT combined with recent turnover in key ISS positions has contributed to the lack of appropriate access

controls. ELECT should align its access process with the Security Standard which will help ensure consistent and appropriate account management and the protection of sensitive information.

Improve Audit Logging and Review Process

ISS Control Area: Audit Logging

ELECT does not implement certain audit logging and monitoring safeguards for a sensitive system in accordance with the Security Standard. We communicated three internal control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard requires audit logging and monitoring controls to protect the confidentiality, integrity, and availability of sensitive and mission-critical data. Due in part to limited personnel resources, ELECT was not able to implement the necessary safeguards described in the FOIAE document and comply with the Security Standard.

ELECT should dedicate the necessary resources to implement the security controls discussed in the communication marked FOIAE in accordance with the Security Standard. Implementing corrective action will help maintain the confidentiality, integrity, and availability of ELECT's sensitive and mission-critical data.

Perform Disaster Recover Testing

ISS Control Area: Risk Management and Contingency Planning

ELECT has not performed an annual exercise of its DRP, as required by the Security Standard. Section CP-1-COV-1 of the Security Standard requires that organizations perform an annual exercise of IT disaster recovery components to assess their adequacy and effectiveness.

ELECT was part of a large disaster recovery exercise through VITA, which was performed by an external vendor. The external vendor was not able to complete testing for ELECT due to problems with ELECT's infrastructure setup. ELECT communicated with VITA to correct the issue; however, the infrastructure correction was not performed in time for a re-test, so testing was not performed.

Without a well-tested DRP, ELECT may not be able to restore the systems that support mission-essential business functions in a timely manner in the event of an emergency or disaster. ELECT should ensure proper communication with VITA to ensure that its infrastructure is appropriately configured for disaster recovery testing and should perform an annual test of disaster recovery components to assess their adequacy and effectiveness.

Department of Energy

Improve Access Controls

ISS Control Area: Access Control

Energy does not have adequate access controls in place to comply with the requirements of the Security Standard. Specifically, Energy has weaknesses in the following areas:

- Energy does not have an adequate process in place for annual review of systems access, as required by the Security Standard, Section AC-2.
- For a sample of six employees whose employment by Energy ended during fiscal year 2019, one employee (17%) did not have access to systems removed within 24 hours of the last day of employment, as required by Section PS-4 of the Security Standard.

Inadequate access controls can result in improper or unnecessary access to sensitive systems, which can lead to a breach in data security. Limited IT personnel and resources contributed to the identified weaknesses; however, Energy is currently working with a third-party provider to improve policies and procedures and align practices with the requirements of the Security Standard. Energy should ensure it communicates the updated policies and procedures throughout the organization to ensure timely access removal following the end of employment and performance of annual access reviews.

Improve Audit Log Monitoring Process

ISS Control Area: Audit Logging

Energy does not implement certain audit logging and monitoring safeguards for sensitive systems that support mission-essential functions in accordance with the Security Standard. We communicated one internal control weakness to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard requires audit logging and monitoring controls to protect the confidentiality, integrity, and availability of sensitive and mission-critical data. Due in part to limited personnel resources, Energy was not able to implement the necessary safeguards described in the FOIAE document and comply with the Security Standard.

Energy should dedicate the necessary resources to implement the security controls discussed in the communication marked FOIAE in accordance with the Security Standard. Implementing corrective action will help maintain the confidentiality, integrity, and availability of Energy's sensitive and mission-critical data.

Improve Disaster Recovery Planning and Testing to Align with the Contingency Plan

ISS Control Area: Risk Management and Contingency Planning

Energy maintains a contingency plan that is in accordance with Section CP1-COV-1 of the Security Standard. The contingency plan includes reference to a separate DRP; however, Energy was unable to provide the referenced DRP or evidence of completed DRP tests.

The Security Standard, Section CP-1-COV-2, requires agencies to develop and maintain a DRP, which is based on the contingency plan and supports the restoration of mission-essential functions and dependent business functions. Additionally, the Security Standard requires the periodic review, reassessment, testing, and revision of the DRP to reflect changes in mission-essential functions, services, IT system hardware and software, and personnel.

Energy has recently made changes to system sensitivity classifications and mission-essential functions, which increases the risk that all necessary components of a DRP are not adequately included in the contingency plan. Limited IT personnel and resources at Energy has contributed to the incomplete DRP and lack of testing. Energy should revise its contingency plan to ensure it includes all required elements of the DRP and it should test the DRP as required by the Security Standard.

Department of Forestry

Improve IT Security Governance

ISS Control Area: Policies and Procedures and IT Governance

Forestry does not have an adequate IT security governance structure to manage its ISS program and comply with the Security Standard. The Security Standard requires the agency to ensure the ISS program is maintained, is adequate to protect the agency's IT systems, and is effectively communicated throughout the organization (Security Standard Section 2.4.2). Specifically, Forestry has weaknesses in the following areas:

- Forestry has not reviewed and updated its information security policies and procedures since 2011, which does not comply with the annual review and update requirement in the Security Standard, Sections AC-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, and SI-1.
- Forestry does not have an ISO that is independent from IT operations, as required in the Security Standard, Section 2.4.1.

An annual review and update of policies and procedures helps ensure that they are reflective of the current information technology environment and comply with the Security Standard. Forestry's lack of review and updates since 2011 increases the risk of noncompliance with the Security Standard and irrelevance of policies and procedures to its information technology environment. By not having an adequate IT security governance structure to properly manage Forestry's IT security program, there is

increased risk that Forestry will not properly secure sensitive IT resources, which can lead to a breach of sensitive data or system unavailability.

Forestry experienced significant turnover in key ISS and management positions, which contributed to the above weaknesses. The current ISO is also the Agency Information Technology Representative (AITR) and as such, cannot provide adequate, independent oversight of IT security. Forestry should establish an independent security function within the organization and integrate IT security with system operations. To reduce any potential conflicts of interest, the ISO should report directly to the agency head, and not the Director of Administration. Forestry should develop a process to review and update ISS policies and procedures at least annually and when significant changes occur. The updated policies and procedures should be communicated throughout Forestry to ensure compliance with the Security Standard.

Improve Access Controls

ISS Control Area: Access Control

Forestry does not have appropriate internal controls to ensure that access to their systems is appropriate and complies with the requirements of the Security Standard. Specifically, Forestry has weaknesses in the following areas:

- Forestry's current access termination process is not adequate to ensure that it removes users' systems access within 24 hours of employment ending, as required by Section PS-4 of the Security Standard. In a sample of five employees whose employment ended during fiscal year 2019, four employees (80%) did not have their systems access removed within 24 hours of their last day of employment.
- Forestry was unable to provide documentation to support an annual review of systems access, as required by the Security Standard, Section AC-2.

Inadequate access controls can result in improper or unnecessary access to sensitive systems, which can lead to a breach in data security. Forestry's limited IT personnel and turnover in key ISS positions are the contributing factors to the internal control weaknesses identified. Forestry should implement improved access controls, to include an annual access review and timely termination process.

Improve Audit Logging Capabilities and Develop a Process for Monitoring Audit Logs

ISS Control Area: Audit Logging and Third-Party Oversight

Forestry has not implemented some required controls for its third-party service providers, as required by the Commonwealth's Hosted Environment Security Standard.

The Hosted Environment Security Standard and best practices require and recommend using specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability. In general, Forestry does not use three required third-party service provider controls. We communicated these

specific internal control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Forestry should review the third-party service providers reports and ensure the configurations, settings, and controls align with the requirements in the Hosted Environment Security Standard and industry best practices. By not meeting the minimum requirements in the Hosted Environment Security Standard, Forestry cannot ensure the confidentiality, integrity, and availability of data within its systems.

Improve Risk Management and Contingency Planning

ISS Control Area: Risk Management and Contingency Planning

Forestry is not properly maintaining IT risk management and contingency planning documentation in accordance with the Security Standard. Our review of Forestry's IT risk management and contingency planning controls identified the following weaknesses:

- Forestry was unable to provide documentation to support IT risk assessments for sensitive systems as required in the Security Standard, Section 6.2.
- Forestry was unable to provide an annual self-assessment of sensitive system IT risk assessments to determine their continued validity as required in the Security Standard, Section 6.2.
- Forestry was unable to provide a BIA as required in the Security Standard, Section 3.2.
- Forestry does not maintain a current continuity of operations and DRP (contingency plan). The provided contingency plan was last updated in 2015 and included reference to retired information systems and other outdated information.
- Forestry is not performing an annual exercise of the IT disaster recovery components of the contingency plan as required in the Security Standard, Section CP1-COV-1.

Forestry has an agreement with a third-party provider (provider) to provide the following deliverables: BIA, system security plan (to include risk assessments and risk treatment plans), and enhanced security services (to include penetration testing, vulnerability assessments, and incident response planning). However, Forestry relies upon the provider to complete these services and does not retain or review deliverables upon their completion.

The Security Standard, Section CP-1-COV-1, requires that agencies use their BIA and risk assessments to develop IT disaster components of the agency contingency plan. These components include identification of each IT system that is necessary to recover agency business functions or dependent business functions and the RTO and RPO for each. Additionally, an annual exercise of DRP components is necessary to assess their adequacy and effectiveness. Forestry experienced turnover in key ISS and management positions which contributed to the identified weaknesses above.

Forestry's current approach to risk management and contingency planning increases the risk that it will not identify and mitigate existing vulnerabilities, which could lead to delays in restoring systems that support mission-critical business functions in the event of an emergency or disaster. Forestry should develop a process to ensure that deliverables completed by the provider are retained and updated in accordance with the Security Standard. Maintaining current risk management and contingency planning documentation will decrease the data security risk for the sensitive systems and improve the overall security of the control environment.

Improve Security Awareness Training Program

ISS Control Area: Security Awareness Training

Forestry is not adequately administering, monitoring, or enforcing annual security awareness training for all information system users. Forestry has not updated its security awareness training program since 2009 and all users have not completed the training as required by the Security Standard.

Section AT-2 of the Security Standard requires agencies to provide basic security awareness training to information system users as part of initial new hire training, when required by information system changes, and annually or more often as necessary thereafter. Additionally, Section AT-4 requires agencies to document and monitor individuals' completion of security awareness training.

Forestry management has required security awareness training to be completed at the start of employment but does not enforce the completion of annual training. Forestry experienced significant turnover in key ISS and management positions, which contributed to management's lack of oversight regarding the annual completion of security awareness training. Without management's enforcement and emphasis on the importance of security awareness training, information system users may lack the knowledge to identify and respond to security threats that could compromise sensitive systems and data. Forestry should update the security awareness training program and ensure information system users complete all elements of the required security awareness training.

Improve Oversight of Third-Party Providers

ISS Control Area: Third-Party Provider Oversight

Forestry is not maintaining proper oversight of providers as required in the Security Standard. The Security Standard, Section 1.1, states that agency heads remain accountable for maintaining compliance with the Security Standard for information technology equipment, systems, and services procured from providers, and agencies must enforce the compliance requirements through documented agreements and oversight of the services provided.

Forestry uses providers to host three of its sensitive information systems supporting mission-essential functions. Forestry was unable to provide documentation to support the performance of the following oversight functions required by Section SA-9-COV-3 of the Hosted Environment Security Standard:

- Perform an annual security audit of the environment or review the annual audit report of the environment conducted by an independent, third-party audit firm on an annual basis.
- Perform a monthly review of activity logs related to the operation of the service.
- Receive vulnerability scans of the operating system and supporting software from the provider at least once every 90-days.

Without a process to gain assurance over providers' operating controls, Forestry cannot validate that those providers have effective security controls for protecting sensitive data increasing risk to information in Forestry and Commonwealth systems. Forestry has experienced significant turnover within key ISS positions along with a lack of IT personnel resources, which are primary factors for not having a process to gain assurance over providers. Forestry should develop a process for ensuring that providers use appropriate security controls and for monitoring the providers as required by the Security Standard.

Department of Health Professions

Improve Communication of Access Controls

ISS Control Area: Access Control

Health Professions does not have appropriate internal controls in place to ensure that access to its systems is appropriate and complies with the requirements of the Security Standard. Health Professions is not removing employee access in a timely manner following termination. In a sample of six employees whose employment ended during fiscal year 2019, two employees (33%) did not have their systems access removed within 24 hours of the end of employment, as required by Section PS-4 of the Security Standard.

The Department of Human Resource Management (Human Resources) provides human resource services, for Health Professions. The Health Professions IT Security Team (IT Security) has not properly communicated the terminations process to supervisors, which has resulted in a misunderstanding between Health Professions' supervisors and Human Resources regarding the responsibility for informing IT Security of terminations. The lack of proper and well-communicated access controls could lead to improper or unnecessary access to sensitive systems and, subsequently, a breach in data security. Health Professions should improve and communicate the process for employee access terminations to both Health Professions' supervisors and Human Resources to ensure that access is removed in a timely manner.

Perform Disaster Recovery Testing

ISS Control Area: Risk Management and Contingency Planning

Health Professions is not adequately testing their DRP. Health Professions has updated the DRP on an annual basis, with the most recent update in February 2020; however, the DRP does not include a documented strategy for disaster recovery testing and the DRP is only tested during when events occur,

such as the COVID-19 pandemic. Section CP-1-COV-1 of the Security Standard requires that agencies perform an annual exercise of IT disaster recovery components to assess their adequacy and effectiveness.

Health Professions is not performing disaster recovery testing due to lack of consistent staffing available during fiscal year 2019. Health Professions had two consecutive emergency coordination officers end employment prior to performing the testing and due to the small size of the agency, the responsibilities associated with that position were not distributed and performed. Without a well-tested DRP, Health Professions may not be able to restore the systems that support mission-critical business functions in a timely manner in the event of an emergency or disaster. Health Professions should develop a process for annual testing of the DRP to ensure the timely restoration of mission-essential functions in the event of a disaster.

Department of Housing and Community Development

Improve IT Governance

ISS Control Area: IT Governance

Housing does not have adequate controls over IT governance, as required by the Security Standard. Specifically, Housing has weaknesses in the following areas:

- Housing does not separate the roles of the ISO and the CIO as required by the Security Standard, Section 2.4.1, which states that the ISO must not simultaneously serve the function of a CIO.
- Housing has not retained the memorandum of understanding (MOU) between Housing and VITA, as required by the Security Standard, Section 1.3, which states that the agency shall maintain documentation regarding specific roles and responsibilities relating to information security.

A lack of separation of duties between the ISO and CIO can lead to inadequate independent oversight of IT security. Additionally, maintaining the MOU between Housing and VITA is essential for the management of the ISS program at the agency, as it identifies the roles and responsibilities of both Housing and VITA. The lack of documentation of the roles and responsibilities of VITA can lead to a misunderstanding of the level of services and lead to IT security requirements not being completed. In addition, without the MOU, Housing cannot ensure that VITA is properly fulfilling all responsibilities as outlined.

Housing has limited technical resources and staff, which has resulted in the assignment of CIO and ISO responsibilities to one individual. Housing was unaware that an exception was required for the same individual to perform the CIO and ISO responsibilities. Housing completed a COV Information Security Policy & Standard Exception Request Form and submitted it to VITA to obtain an exception to the Security Standard, Section 2.4.1. Housing should obtain the approved exception from VITA and work toward obtaining the necessary resources to allow for a separation between the CIO and ISO.

The MOU between Housing and VITA was signed and maintained by an employee that is no longer with Housing. Housing has requested a copy of the MOU from VITA. Housing should obtain the MOU from VITA and ensure it retains the MOU in its ISS program documentation. Housing should review the MOU to ensure all responsibilities are being performed by the appropriate parties.

Improve Controls over Access Removal for Terminated Employees

ISS Control Area: Access Control

Housing does not have adequate internal controls in place to ensure that access termination complies with the requirements of the Security Standard. In a sample of three employees whose employment by Housing ended during fiscal year 2019, one employee (33%) did not have access to systems removed within 24 hours of the last day of employment, as required by Section PS-4 of the Security Standard. Housing submitted the request to remove system access five days following the employee's last day of employment.

The individual responsible for submitting the system access removal request was out of the office on the day of the employee's separation and no backup was identified. As such, the responsible individual submitted the system access removal request upon returning to the office. Delays in access removal put Housing at risk due to inappropriate system access, which can compromise the security of sensitive data.

Housing should identify and assign another individual to serve as a backup to submit requests to remove system access when the primary individual is out of the office. Housing should document this process within its policies and procedures and communicate it to all appropriate individuals within the agency.

Department of Juvenile Justice

Update Policies and Procedures

ISS Control Area: Policies and Procedures

Juvenile Justice is not adequately reviewing its IT policies and procedures. The Security Standard requires that agencies perform a review of IT policies on an annual basis or more frequently, if required to address an environmental change, to assess their adequacy and effectiveness. Juvenile Justice has not reviewed its IT policies and procedures since 2016 or earlier.

The absence of annual policy and procedure reviews is due to a lack of management oversight and turnover within key information security positions. The current ISO took the position at the beginning of fiscal year 2019 and has been working to improve Juvenile Justice's IT environment. Juvenile Justice's IT policies and procedures are reasonably aligned with the Security Standard; however, an annual review process will decrease the risk of noncompliance with the Security Standard and ensure alignment of policies and procedures with the current IT environment.

Improve Access Controls

ISS Control Area: Access Control

Juvenile Justice does not have appropriate internal controls in place to ensure access to its systems is appropriate and complies with the requirements of the Security Standard. Specifically, Juvenile Justice has weaknesses in the following areas:

- Juvenile Justice's access termination process is not adequate to ensure systems access is removed within 24 hours of an employee's last day of employment, as required by Section PS-4 of the Security Standard. For a sample of 25 employees whose employment by Juvenile Justice ended during fiscal year 2019, 12 employees (48%) did not have their systems access removed within 24 hours of their last day of employment, while six had no documentation to support the removal of systems access.
- Juvenile Justice was unable to provide documentation to support an annual review of systems access, as required by the Security Standard, Section AC-2.

Inadequate access controls can result in improper or unnecessary access to sensitive systems, which can lead to a breach in data security. Juvenile Justice's internal policies and procedures include access controls which align with the Security Standard; however, a lack of management oversight during fiscal year 2019 contributed to the internal control weaknesses identified. Juvenile Justice should implement improved access controls, which align practices with the Security Standard, to include an annual access review and timely access termination process.

Improve Process for Reviewing Audit Logs

ISS Control Area: Audit Logging

Juvenile Justice does not implement certain audit logging and monitoring safeguards for sensitive systems that support mission-essential functions in accordance with the Security Standard. We communicated two internal control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard requires audit logging and monitoring controls to protect the confidentiality, integrity, and availability of sensitive and mission-critical data. Due in part to limited personnel resources, Juvenile Justice was not able to implement the necessary safeguards described in the FOIAE document and comply with the Security Standard.

Juvenile Justice should dedicate the necessary resources to implement the security controls discussed in the communication marked FOIAE in accordance with the Security Standard. Implementing corrective action will help maintain the confidentiality, integrity, and availability of Juvenile Justice's sensitive and mission-critical data.

Update Risk Assessment and Contingency Planning

ISS Control Area: Risk Management and Contingency Planning

Juvenile Justice is not properly maintaining IT risk management and contingency planning documentation in accordance with the Security Standard. Our review of Juvenile Justice's IT risk management and contingency planning controls identified the following weaknesses.

- Juvenile Justice was unable to provide documentation to support IT risk assessments for sensitive systems as required in the Security Standard, Section 6.2.
- Juvenile Justice was unable to provide an annual self-assessment of sensitive system IT risk assessments to determine their continued validity as required in the Security Standard, Section 6.2.
- Juvenile Justice was unable to provide a BIA as required in the Security Standard, Section 3.2.
- Juvenile Justice does not maintain a current IT contingency plan.
- Juvenile Justice is not performing an annual exercise of the IT disaster recovery components of the contingency plan as required in the Security Standard, Section CP1-COV-1.

Juvenile Justice has an agreement with a provider for the following deliverables: BIA, system security plan (to include risk assessments and risk treatment plans), and enhanced security services (to include penetration testing, vulnerability assessments, and incident response planning). However, Juvenile Justice relies upon the provider to complete these services and does not retain or review deliverables upon their completion.

The Security Standard, Section CP-1-COV-1, requires that agencies use their BIA and risk assessments to develop IT disaster components of the agency contingency plan. These components include identification of each IT system that is necessary to recover agency business functions or dependent business functions and the RTO and RPO for each. Additionally, an annual exercise of DRP components is necessary to assess their adequacy and effectiveness. A lack of management oversight and turnover within key ISS positions contributed to the weaknesses identified above.

Juvenile Justice's current approach to risk management and contingency planning increases the risk that it will not identify and mitigate existing vulnerabilities, which could lead to delays in restoring systems that support mission-critical business functions in the event of an emergency or disaster. Juvenile Justice should develop a process to ensure that it retains and updates deliverables completed in accordance with the Security Standard. Maintaining current risk management and contingency planning documentation will decrease the data security risk for the sensitive systems and improve the overall security of the control environment.

Perform IT Security Audits

ISS Control Area: Risk Management and Contingency Planning

Juvenile Justice does not have an adequate process to provide for IT security audits for its sensitive systems, as required by the Security Standard. The Security Standard, Section 1.4, requires that, at a minimum, IT systems that contain sensitive data or reside in a system with high sensitivity be assessed at least once every three years. Juvenile Justice last received an audit of its sensitive systems in 2016.

Due to turnover in key ISS positions and overall lack of management oversight, Juvenile Justice did not obtain IT security audits within the past three years. IT security audits help ensure that IT system controls are adequate and ensure compliance with established IT security policy and procedures. A lack of regular IT security audits for sensitive systems may result in unidentified system vulnerabilities and noncompliance with the Security Standard. Juvenile Justice should ensure that it obtains IT security audits at least once every three years and that it addresses any findings as necessary.

Perform Annual Security Awareness Training

ISS Control Area: Security Awareness Training

Juvenile Justice is not providing annual security awareness training to employees. Section AT-1 of the Security Standard requires agencies to develop, update, and distribute security awareness training to all information system users on an annual basis.

Due to a lack of management oversight and turnover within key ISS positions, Juvenile Justice is not providing security awareness training to information system users. The current ISO began employment at the beginning of fiscal year 2019 and has been working to improve Juvenile Justice's information technology environment. Information system users who do not complete security awareness training annually may lack the knowledge to identify and respond to security threats that could compromise sensitive systems and information. Juvenile Justice should develop and implement a security awareness training program and ensure that all information system users complete the training annually as required by the Security Standard.

Department of Labor and Industry

Improve Controls over Access Removal for Terminated Employees

ISS Control Area: Access Control

Labor and Industry does not have adequate internal controls in place to ensure access termination complies with the requirements of the Security Standard. For a sample of four employees whose employment by Labor and Industry ended during fiscal year 2019, one employee (25%) did not have access to systems removed within 24 hours of the last day of employment, as required by Section PS-4 of the Security Standard. Labor and Industry removed the employee's access three days after the last day of employment.

Labor and Industry's access termination policy states that access should be removed within 24 hours of notification, but the employee's manager did not notify the IT Department of the employee's separation until several days following the employee's last day. The delay in removing the employee's access was the result of an unclear policy and lack of agency understanding of the requirement to terminate access within 24 hours of the last day of employment. Delays in access removal put Labor and Industry at risk due to inappropriate system access, which could compromise the security of sensitive data. Labor and Industry should revise its policy to ensure that it clearly notes that systems access should be removed within 24 hours of an employee's separation and should communicate the requirement throughout the agency.

Improve Process for Reviewing Audit Logs

ISS Control Area: Audit Logging

Labor and Industry does not implement certain audit logging and monitoring safeguards for sensitive systems that support mission-essential functions in accordance with the Security Standard. We communicated two internal control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard requires audit logging and monitoring controls to protect the confidentiality, integrity, and availability of sensitive and mission-critical data. Due in part to limited personnel resources, Labor and Industry was not able to implement the necessary safeguards described in the FOIAE document and comply with the Security Standard.

Labor and Industry should dedicate the necessary resources to implement the security controls discussed in the communication marked FOIAE in accordance with the Security Standard. Implementing corrective action will help maintain the confidentiality, integrity, and availability of Labor and Industry's sensitive and mission-critical data.

Perform Disaster Recovery Testing

ISS Control Area: Risk Management and Contingency Planning

Labor and Industry is not properly testing its DRP, as required by the Security Standard. Section CP-1-COV-1 of the Security Standard requires that agencies perform an annual exercise of IT disaster recovery components to assess their adequacy and effectiveness.

Labor and Industry has experienced turnover in the Continuity Coordinator position, which resulted in it not testing its DRP for several years. Without a well-tested DRP, Labor and Industry may not be able to restore the systems that support mission-critical business functions in a timely manner in the event of an emergency or disaster. Labor and Industry should institute a process for annual testing of the DRP to ensure timely restoration of mission-essential functions in the event of a disaster.

Department of Military Affairs

Improve Access Controls

ISS Control Area: Access Control

Military Affairs does not have a sufficient process in place to ensure removal of system access following employee departures from the agency. Military Affairs operates under the Virginia Army National Guard network, which has established internal cybersecurity policies in accordance with applicable Army regulations and Department of Defense guidance. Military Affairs was unable to provide sufficient documentation to support access removal following the end of employment for two of the seven (29%) employees sampled. This finding resulted from staff turnover in the IT area.

Lack of documentation to support timely access removal following an employee's last day of employment increases the risk that a user retains inappropriate access, which could lead to unauthorized access to sensitive information. Military Affairs internal cybersecurity policies include an out-processing checklist which includes consideration of access removal following the employee's separation date. Military Affairs should follow their processes over access removal following the end of employment to ensure proper completion of out-processing procedures as noted in the cybersecurity policy. Timely removal of unnecessary access will help protect the confidentiality, availability, and integrity of information.

Improve Risk Management and Contingency Planning

ISS Control Area: Risk Management and Contingency Planning

Military Affairs was unable to provide sufficient documentation to support proper risk management and IT contingency planning. Military Affairs maintains an IT contingency plan that is in accordance with the requirements of Department of the Army Pamphlet 25 – 1 – 2 (DA PAM 25 – 1 – 2). However, Military Affairs was unable to provide a risk management plan and business impact analysis as required by Chapters 3 – 4 and 3 – 5 of DA PAM 25 – 1 – 2. This finding resulted from staff turnover in the IT area.

Military Affairs should conduct both a risk management plan and business impact analysis to help in identifying critical processes and areas of risk to support IT contingency planning. Maintaining a risk management plan and business impact analysis will decrease the data security risk for sensitive systems and improve the overall security of the control environment.

Department of Professional and Occupational Regulation

Improve IT Security Governance

ISS Control Area: Policies and Procedures and IT Governance

Professional and Occupational Regulation does not have an adequate IT security governance structure to manage its ISS program and comply with the Security Standard. Specifically, Professional and Occupational Regulation has weaknesses in the following areas:

- Professional and Occupational Regulation does not have an ISO that is independent from IT operations, as required in the Security Standard, Section 2.4.1.
- Professional and Occupational Regulation does not annually update ISS policies and procedures as required in the Security Standard, Sections AC-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, and SI-1.

Due to Professional and Occupational Regulation's limited IT personnel and resources, the ISO reports to the AITR. Limited IT personnel and resources also resulted in Professional and Occupational Regulation not properly updating its policies and procedures. The current reporting structure increases the risk that Professional and Occupational Regulation will not properly secure sensitive IT resources, which can lead to a breach of sensitive data or system unavailability. Additionally, Professional and Occupational Regulation's lack of annual review and update of policies, as required by the Security Standard, leads to an increase in the risk of noncompliance with Security Standard requirements. Out of date policies and procedures can result in insufficient or inappropriate processes and leave the agency at risk for improper system usage.

To reduce potential conflicts of interest, Professional and Occupational Regulation should modify the reporting structure to ensure that the ISO reports directly to the agency head, and not the AITR. Additionally, management should develop a process to ensure that policies and procedures are reviewed and updated annually, or more frequently to address environmental changes. Professional and Occupational Regulation should communicate the updated policies and procedures throughout the agency to ensure compliance with the Security Standard requirements.

Improve Audit Logging and Monitoring Process

ISS Control Area: Audit Logging

Professional and Occupational Regulation does not implement certain audit logging and monitoring safeguards for mission-essential sensitive systems in accordance with the Security Standard. We communicated one internal control weakness to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard requires audit logging and monitoring controls to protect the confidentiality, integrity, and availability of sensitive and mission-critical data. Due in part to limited personnel resources, Professional and Occupational Regulation was not able to implement the necessary safeguards described in the FOIAE document and comply with the Security Standard.

Professional and Occupational Regulation should dedicate the necessary resources to implement the security controls discussed in the communication marked FOIAE in accordance with the Security Standard. Implementing corrective action will help maintain the confidentiality, integrity, and availability of Professional and Occupational Regulation's sensitive and mission-critical data.

Ensure IT Security Audits are Performed

ISS Control Area: Risk Management and Contingency Planning

Professional and Occupational Regulation does not have an adequate process in place to obtain IT security audits for its sensitive systems, as required by the Security Standard. The Security Standard, Section 1.4, requires that at a minimum, IT systems that contain sensitive data, or reside in a system with high sensitivity, be assessed at least once every three years. Professional and Occupational Regulation last received an audit over its three sensitive systems in 2016.

Due to turnover in key ISS positions and overall lack of management oversight, Professional and Occupational Regulation did not ensure completion of an IT security audit within the past three years. IT security audits help ensure that IT system controls are adequate and ensure compliance with established IT security policy and procedures. A lack of regular IT security audits for sensitive systems may result in unidentified system vulnerabilities and noncompliance with the Security Standard. Professional and Occupational Regulation should ensure completion of IT Security audits at least once every three years and appropriate address any findings as necessary.

Improve Security Awareness Training Process

ISS Control Area: Security Awareness Training

Professional and Occupational Regulation is not properly monitoring the completion of annual security awareness training for all information system users. Section AT-2 of the Security Standard requires agencies to provide basic security awareness training to information system users as part of initial new-hire training, when required by information system changes, and annually or more often as necessary thereafter. Additionally, Section AT-4 requires agencies to document and monitor individuals' completion of security awareness training.

Due to lack of management oversight, six percent of employees, did not complete security awareness training. Without annual security awareness training, information system users may lack the knowledge to identify and respond to security threats that could compromise sensitive systems and data. Professional and Occupational Regulation should improve its monitoring process to ensure all information system users complete security awareness training annually as required by the Security Standard.

Department of Small Business and Supplier Diversity

Improve Audit Log Controls

ISS Control Area: Audit Logging

Small Business does not have adequate internal controls over the audit logging process, as required by Hosted Environment Security Standard. Specifically, Small Business has weaknesses in the following areas:

- Small Business does not document its weekly review and analysis of information system audit records for indications of inappropriate or unusual activity as required by the Hosted Environment Security Standard, Section AU-6.
- Small Business's audit record review does not contain the audit events identified in the Hosted Environment Security Standard, Sections AU-2 and SA-9-COV-3.

Small Business relies on the system host to perform audit log monitoring and receives weekly reports of vulnerability testing. A lack of documentation of the audit record review and necessary audit events increases the risk of undetected audit events and security incidents. Small Business should develop a process to ensure it reviews sensitive system audit records weekly and should retain documentation of audit record reviews. Small Business should ensure the audit records include all audit events identified in the Hosted Environment Security Standard, Sections AU-2 and SA-9-COV-3.

Perform Disaster Recovery Testing

ISS Control Area: Risk Management and Contingency Planning

Small Business is not properly testing its DRP as required by the Security Standard. Section CP-1-COV-1 of the Security Standard requires that agencies perform an annual exercise of IT disaster recovery components to assess their adequacy and effectiveness. Small Business did not have a clear understanding of the services provided by VITA and believed they included DRP testing.

Without a well-tested DRP, Small Business may not be able to restore the systems that support mission-critical business functions promptly in the event of an emergency or disaster. Small Business should institute a process for annual testing of its DRP to ensure timely restoration of mission-essential functions in the event of a disaster.

Indigent Defense Commission

Strengthen Policies and Procedures

ISS Control Area: Policies and Procedures

The Defense Commission does not have adequate policies and procedures to comply with the Security Standard. The Security Standard, Section 2.4.2, requires that an ISS program is maintained, is adequate to protect IT systems, and is effectively communicated throughout the organization.

Additionally, while the Defense Commission does have some policies and procedures documented, they do not include all required elements of the Security Standard. The Defense Commission has weaknesses in the following areas:

- Section AC-1 requires an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination, and compliance as well as procedures to facilitate the implementation of the policy and associated controls. The

Defense Commission's policies include initial access request procedures but do not speak to access modification, termination, or review.

- Section AU-6 requires agencies to review and analyze information system audit records at least every 30-days for indications of inappropriate or unusual activity. The Defense Commission has processes in place to notify IT staff of unusual activity and threats; however, there are no policies and procedures documented for the review of unusual activity that is logged within information systems.
- Section IA-5 requires management to enforce system password changes every 90 days. The Defense Commission's password management policy does not include requirements related to changing passwords as required by the Security Standard.

The Defense Commission's lack of IT personnel resources, and corresponding constraints on their time, is a primary cause for not having adequate policies and procedures over ISS. The Defense Commission's lack of adequate policies and procedures increases the risk of improperly securing or using IT resources. The Defense Commission should work to strengthen its policies and procedures to ensure compliance with the Security Standard and should review and update them annually to address any environmental changes.

Improve Controls over Access Removal for Terminated Employees

ISS Control Area: Access Control

The Defense Commission does not have adequate internal controls in place to ensure that access to systems is appropriate and complies with the requirements of the Security Standard. For a sample of ten employees whose employment by the Defense Commission ended during fiscal year 2019, two employees (20%) did not have their systems access removed within 24 hours of their last day of employment, as required by Section PS-4 of the Security Standard. The Defense Commission submitted the requests to remove system access for each employee between four to seven days following the last date of employment. Additionally, the Defense Commission's most recent systems access review resulted in the removal of 34 accounts across four systems due to inactivity or prior termination of employment.

The Defense Commission has an offboarding checklist to follow when removing access for all systems but does not have adequate policies governing the removal of systems access. Additionally, the current access termination process is not adequate to ensure that the Defense Commission removes systems access within 24 hours of an employee's last date of employment.

The lack of documented policies surrounding access terminations puts the Defense Commission at risk of inappropriate system access, which could compromise the security of sensitive data. Management should develop and implement policies surrounding employee access termination and should educate all systems management employees on the process to ensure timely access termination.

Ensure Completion and Validity of Risk Assessments*ISS Control Area: Risk Management and Contingency Planning*

The Defense Commission was not able to provide risk assessments for all sensitive systems. Section 6.2 of the Security Standard requires agencies to conduct and document a risk assessment of each sensitive IT system at least once every three years. Additionally, the Security Standard requires agencies to conduct and document an annual self-assessment to determine the continued validity of risk assessments and to prepare a report of each risk assessment that includes identification of all vulnerabilities discovered during the self-assessment and an executive summary, including major findings and risk mitigation recommendations.

The Defense Commission has a contract with a third-party provider to complete risk assessments for all sensitive systems; however, the Defense Commission relies upon the provider to perform the risk assessments and does not retain or review the risk assessments upon their completion. Additionally, the Defense Commission does not perform annual self-assessments to ensure the continued validity of the risk assessments and does not prepare a report of the risk assessments that identifies the vulnerabilities and an executive summary of major findings and risk mitigation recommendations.

The Defense Commission's current approach to risk assessments increases the risk that it will not identify and mitigate existing vulnerabilities. The Defense Commission should develop a process to ensure that after the provider completes a risk assessment for each sensitive system, the Defense Commission obtains and retains a copy, and reviews and updates the risk assessment on an annual basis or after any significant changes. Maintaining current risk assessments will decrease the data security risk for the sensitive systems and improve the overall security of the control environment.

Perform Disaster Recovery Testing*ISS Control Area: Risk Management and Contingency Planning*

The Defense Commission is not adequately reviewing and testing its DRP. The Defense Commission implemented its DRP in 2014 and did not review and update the plan until 2020. In addition, the Defense Commission is only testing the DRP during live exercises, such as firewall failovers and network interruptions. Section CP-1-COV-1 of the Security Standard requires that agencies perform an annual exercise of DRP components to assess their adequacy and effectiveness. Further, Section CP-2 of the Security Standard requires that the IT contingency plan be reviewed and updated on an annual basis, or more frequently if required to address an environmental change.

The Defense Commission does not have sufficient IT personnel resources to ensure that it reviews and tests the DRP on an annual basis, which has resulted in the agency's reliance on live disaster recovery tests. Without an updated and well-tested DRP in place, the Defense Commission may not be able to restore the systems that support mission-critical business functions in a timely manner in the event of an emergency or disaster. The Defense Commission should allocate adequate resources to disaster recovery planning and testing within its administrative and field offices. Additionally, the Defense Commission should institute a process for annual review and testing of the DRP to ensure the timely restoration of mission-essential functions in the event of a disaster.

Improve Oversight of Third-Party Providers

ISS Control Area: Third-Party Provider Oversight

The Defense Commission uses providers to provide and host several information systems that support its mission-critical business functions. The Defense Commission does not have a process in place to gain assurance that providers have adequate security controls to protect sensitive data. The Defense Commission does not perform the following oversight functions as required by section SA-9-COV-3 of the Hosted Environment Security Standard:

- Perform an annual security audit of the environment or review the annual audit report of the environment conducted by an independent, third-party audit firm on an annual basis.
- Perform a monthly review of activity logs related to the operation of the service.
- Receive vulnerability scans of the operating system and supporting software from the provider at least once every 90-days.

Section 1.1 of the Hosted Environment Security Standard states that the agency head is accountable for maintaining and enforcing compliance with the standard through documented agreements with providers and oversight of the services provided. Without a process to gain assurance over providers' operating controls, the Defense Commission cannot validate that those providers have effective security controls for protecting sensitive data, which puts the Defense Commission's, and therefore the Commonwealth's, information at risk. The Defense Commission's lack of IT personnel resources, and corresponding constraints on their time, is a primary contributor for not having a process to gain assurance over providers.

Management should consider developing and implementing a process to maintain oversight of providers. Developing and implementing an oversight process provides the Defense Commission with assurance over the confidentiality, availability, and integrity of systems which support mission-critical business functions.

Jamestown-Yorktown Foundation

Improve Access Controls

ISS Control Area: Access Control

The Foundation does not employ appropriate internal controls to ensure that access to its systems is appropriate and complies with the requirements of the Security Standard. Specifically, the Foundation has weaknesses in the following areas:

- The Foundation does not have adequate policies and procedures governing the removal of systems access and the current access termination process is not adequate to ensure that systems access is removed within 24 hours of termination, as required by Section PS-4 of the

Security Standard. For a sample of six employees whose employment by the Foundation ended during fiscal year 2019, three employees (50%) did not have their systems access removed within 24 hours of the end of employment.

- The Foundation does not have a process in place for an annual review of systems access, as required by the Security Standard, Section AC-2.
- The Foundation has not configured its information systems to ensure that it disables inactive accounts after 90 consecutive days of inactivity as required by the Security Standard, Section AC-2.

Inadequate access controls can result in improper or unnecessary access to sensitive systems, which can lead to a breach in data security. The Foundation's limited IT personnel and use of hardcopy account management requests are the contributing factors to the internal control weaknesses identified. The Foundation should implement improved access controls, to include an annual access review and timely access termination process. In addition, the Foundation should consider automating access control processes to promote timely access termination and review of systems access and to disable inactive accounts after 90 days of inactivity.

Improve Audit Logging Capabilities and Develop a Process for Monitoring Audit Logs

ISS Control Area: Audit Logging

The Foundation does not implement certain audit logging and monitoring safeguards for sensitive systems that support mission-essential functions in accordance with the Security Standard. We communicated three internal control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard requires audit logging and monitoring controls to protect the confidentiality, integrity, and availability of sensitive and mission-critical data. Due in part to limited resources, the Foundation was not able to implement the necessary safeguards described in the FOIAE document and comply with the Security Standard.

The Foundation should dedicate the necessary resources to implement the security controls discussed in the communication marked FOIAE in accordance with the Security Standard. Implementing corrective action will help maintain the confidentiality, integrity, and availability of the Foundation's sensitive and mission-critical data.

Perform IT Disaster Recovery Testing

ISS Control Area: Risk Management and Contingency Planning

The Foundation is not adequately testing its DRP. The Foundation maintains a comprehensive contingency plan, which includes adequate DRP components. However, the Foundation does not properly include components of the DRP in its annual testing of the contingency plan. Section CP-1-COV-

1 of the Security Standard requires that agencies perform an annual exercise of DRP components to assess their adequacy and effectiveness.

The Foundation relies on nightly off-site system back-ups performed by a third party to recover data in the event of a disaster but does not regularly test the IT components of the DRP. The Foundation has limited information security personnel and resources, which has resulted in the DRP not being adequately tested. Without a well-tested DRP, the Foundation may not be able to restore the systems that support mission-critical business functions in a timely manner in the event of an emergency or disaster. The Foundation should implement a process for including the DRP components of the contingency plan in the annual test as required by the Security Standard.

Ensure Completion and Validity of Risk Assessments

ISS Control Area: Risk Management and Contingency Planning

The Foundation was not able to provide risk assessments for all sensitive systems. The Foundation has a contract with a provider to complete a risk assessment for each sensitive system but does not retain or review the risk assessments upon their completion.

Section 6.2 of the Security Standard requires agencies to conduct and document a risk assessment of each sensitive IT system at least once every three years. Additionally, the Security Standard requires agencies to conduct and document an annual self-assessment to determine the continued validity of risk assessments and to prepare a report of each risk assessment that includes identification of all vulnerabilities discovered during the self-assessment and an executive summary, including major findings and risk mitigation recommendations.

Due to the Foundation's limited IT resources, the provider developed a risk assessment plan with the Foundation to ensure performance of the risk assessments as required. However, the Foundation does not have an appropriate process to ensure that the current risk assessments are available for use in completing the BIA and addressing system vulnerabilities. The Foundation's current approach to risk assessments increases the risk that it will not identify and mitigate existing vulnerabilities. The Foundation should develop a process to ensure that after the provider completes a risk assessment for each sensitive system, the Foundation obtains and retains a copy, and reviews and updates the risk assessment on an annual basis or after any significant changes. Maintaining current risk assessments will decrease the data security risk for the sensitive systems and improve the overall security of the control environment.

Improve Security Awareness Training Program

ISS Control Area: Security Awareness Training

The Foundation is not adequately administering, monitoring, or enforcing annual security awareness training for all information system users. During fiscal year 2019, the Foundation did not provide a consistent security awareness training program that included all the Security Standard requirements to all users. The Foundation requires training to be completed upon hiring and annually

thereafter; however, less than 30 percent of required employees completed training during fiscal year 2019.

Section AT-2 of the Security Standard requires the Foundation to provide basic security awareness training to information system users as part of initial new hire training, when required by information system changes, and annually or more often as necessary thereafter. Additionally, Section AT-4 requires the Foundation to document and monitor individuals' completion of security awareness training.

The Foundation's attitudes toward security awareness training do not emphasize the value or necessity of the training. Due to this tone at the top, security awareness training is not a priority and has not been properly administered and enforced. Without management's enforcement and emphasis on the importance of security awareness training, information system users may lack the knowledge to identify and respond to security threats that could compromise sensitive systems and data. The Foundation should reiterate the importance of security awareness training to all information system users and should improve upon the process to ensure that all information system users are completing all elements of the required security awareness training.

Ensure Proper Oversight of Third-Party Providers

ISS Control Area: Third-Party Provider Oversight

The Foundation does not have a formal process to manage third-party Software as a Service (SaaS) providers that fall under VITA's ECOS. The Foundation uses VITA's ECOS to assist in gaining assurance that its SaaS providers implement the minimum-security requirements required by the Hosted Environment Security Standard. The Hosted Environment Security Standard, Section 1.1, states that management remains accountable for maintaining compliance with the Hosted Environment Security Standard through documented agreements and oversight of services provided.

The Foundation signed an MOU with VITA's ECOS to include supply chain management services and cloud oversight and governance. Under this MOU, VITA's ECOS is responsible for performance monitoring, service-level agreement management, operational oversight, and security conformance of off-premise-based systems and services offered by third-party SaaS providers. Due to the Foundation's lack of understanding of its roles and responsibilities, the Foundation has not ensured that VITA's ECOS communicates with its SaaS providers to obtain the cloud oversight and governance deliverables as outlined in the MOU. Therefore, the Foundation has not reviewed the proper documentation to ensure the SaaS providers' compliance with the Hosted Environment Security Standard.

Without a formal process to review and maintain VITA's ECOS documentation, the Foundation cannot validate whether its SaaS providers implement security controls that meet the requirements in the Hosted Environment Security Standard to protect the agency's sensitive and confidential data. The Foundation should develop a formal process to monitor and maintain oversight of its third-party SaaS providers to ensure they comply with the Hosted Environment Security Standard and that VITA's ECOS is meeting all requirements in the MOU. These measures will help maintain the confidentiality, integrity, and availability of sensitive and mission-critical data.

Office of the State Inspector General

Perform Disaster Recover Testing

ISS Control Area: Risk Management and Contingency Planning

Inspector General is not adequately testing its DRP. Inspector General implemented the DRP in 2017 and has performed annual reviews as required but does not properly include the DRP components in its annual contingency plan testing. Inspector General conducted system restores as part of regular business functions and was using these incidents to assess system recovery capabilities. Section CP-1-COV-1 of the Security Standard requires that agencies perform an annual exercise of DRP components to assess their adequacy and effectiveness.

Inspector General is not performing dedicated disaster recovery testing due to lack of understanding that normal restores are not sufficient to satisfy the requirements of the Security Standard. Without a well-tested DRP in place, Inspector General may not be able to restore the systems that support mission-critical business functions in a timely manner in the event of an emergency or disaster. Inspector General should develop a process for annual testing of the DRP to ensure the timely restoration of mission-essential functions in the event of a disaster.

State Council of Higher Education for Virginia

Develop and Implement Policies and Procedures

ISS Control Area: Policies and Procedures

SCHEV does not have policies and procedures over ISS. The Security Standard, Sections AC-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, RA-1, SA-1, SC-1, and SI-1, requires that agencies maintain policies and procedures over various areas of ISS.

SCHEV has a small ISS staff, which has contributed to the lack of policies and procedures. A lack of policies and procedures surrounding ISS may result in insufficient or inappropriate processes and leaves the agency at risk for improper system usage due to lack of formal guidance. SCHEV is in the process of developing policies and procedures and should finalize and implement those policies and procedures to ensure that the agency's information system processes align with the requirements of the Security Standard.

Improve Access Controls

ISS Control Area: Access Control

SCHEV does not have appropriate internal controls in place to ensure that access to its systems is appropriate and complies with the requirements of the Security Standard. Specifically, SCHEV has weaknesses in the following areas:

- SCHEV's current access termination process is not adequate to ensure that systems access is removed within 24 hours of employment ending, as required in Section PS-4 of the Security

Standard. SCHEV was unable to provide documentation to support timely access termination for the three employees whose employment by SCHEV ended during fiscal year 2019.

- SCHEV does not have a process in place for an annual review of systems access as required by the Security Standard, Section AC-2.

Without reviewing all accounts on an annual basis, SCHEV cannot verify that each user's access is appropriate based on job functions, does not violate the principles of least privilege or separation of duties, and is configured appropriately. Lack of documentation to support timely access removal following termination combined with the lack of an access review increases the risk that a user retains inappropriate access, which could lead to unauthorized access to sensitive information.

SCHEV has a small ISS staff and has been in the process of revamping its ISS processes but has not implemented an annual access review or formal access termination process. SCHEV should develop a formal access termination process to ensure it removes access timely and adequately documents access removal. SCHEV should also develop an annual access review process to ensure that access to systems is reasonable and appropriate to protect the confidentiality, availability, and integrity of the information within the systems.

Improve Audit Logging Process

ISS Control Area: Audit Logging

SCHEV does not implement certain audit logging and monitoring safeguards for mission-essential sensitive systems in accordance with the Security Standard. We communicated three control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard requires audit logging and monitoring controls to protect the confidentiality, integrity, and availability of sensitive and mission-critical data. Due in part to limited personnel resources, SCHEV was not able to implement the necessary safeguards described in the FOIAE document and comply with the Security Standard.

SCHEV should dedicate the necessary resources to implement the security controls discussed in the communication marked FOIAE in accordance with the Security Standard. Implementing corrective action will help maintain the confidentiality, integrity, and availability of SCHEV's sensitive and mission-critical data.

Update Contingency Plans and Perform Disaster Recovery Testing

ISS Control Area: Risk Management and Contingency Planning

SCHEV has not identified all information systems with an RTO and RPO or a plan for DRP testing in its contingency planning documents and has not performed an IT disaster recovery test. The Security Standard, Section CP-1-COV-1, requires that agencies develop IT disaster components of the agency contingency plan which identifies each IT system that is necessary to recover agency business functions

or dependent business functions and the RTO and RPO for each. Section CP-1-COV-1 also requires an annual exercise (or more often as necessary) of the DRP components to assess their adequacy and effectiveness.

SCHEV has a small ISS staff, which has been in the process of revising and improving the ISS program but has not yet updated the IT components of the contingency plan or performed DRP testing. Without an updated and well-tested DRP, SCHEV may not be able to restore the systems that support mission-critical business functions in a timely manner in the event of an emergency or disaster. SCHEV should allocate adequate resources to disaster recovery planning and testing and should institute a process for annual review and testing of the IT components of its contingency plans to ensure the timely restoration of mission-essential functions in the event of a disaster.

Improve Security Awareness Training

ISS Control Area: Security Awareness Training

SCHEV does not have an adequate process in place to ensure that all information system users complete annual security awareness training. Of the 59 agency employees, five (8%) did not complete security awareness training during fiscal year 2019. The Security Standard, Section AT-2, requires that the organization provide security awareness training as part as initial training for new users, when required by information system changes, and annually or more often as necessary thereafter.

SCHEV has a small ISS staff, which has resulted in a lack of monitoring annual security awareness training. Information system users who do not complete security awareness training annually may lack the knowledge to identify and respond to security threats that could compromise sensitive systems and information. SCHEV should ensure that all information system users are completing all elements of the required security awareness training and should consider disabling account access if users do not complete training.

Virginia Museum of Natural History

Improve IT Security Governance

ISS Control Area: Policies and Procedures and IT Governance

Natural History does not have an adequate IT security governance structure to manage its ISS program and comply with the Security Standard. The Security Standard, Section 2.4.1, requires the agency to ensure the ISS program is maintained, is adequate to protect the agency's IT systems, and is effectively communicated throughout the organization. Specifically, Natural History has weaknesses in the following areas:

- Natural History does not have an internal full-time ISO that is independent from museum operations and reports to the agency head, as required in the Security Standard, Section 2.4.1.

- Natural History has not performed annual updates of policies and procedures in place related to ISS, as required in the Security Standard, Sections AC-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, and SI-1.

Natural History has not allocated appropriate personnel resources to the information security program, which has resulted in the distribution of ISS responsibilities to various departments and the agency not properly updating policies and procedures. The current ISO is also a trades technician within the Building and Grounds Department, and cannot provide adequate, independent oversight of IT security. By not having an adequate IT security governance structure to properly manage Natural History's IT security program, there is increased risk that Natural History will not properly secure sensitive IT resources, which can lead to a breach of sensitive data or system unavailability.

Natural History should establish an independent ISS function within the organization and integrate IT security with system operations. To reduce any potential conflicts of interest, the ISO should report directly to the agency head, and not the Building and Grounds Manager. Natural History should update policies and procedures annually in accordance with the Security Standard. Finally, Natural History should evaluate its IT resource levels to ensure sufficient resources are available to implement any IT security governance changes and remediate any internal control deficiencies. Improving the IT governance structure will help ensure the confidentiality, integrity, and availability of sensitive data.

Improve Access Controls

ISS Control Area: Access Control

Natural History does not have appropriate internal controls in place to ensure access to its systems is appropriate and complies with the requirements of the Security Standard. Specifically, Natural History has weaknesses in the following areas:

- Natural History's current access termination process is not adequate to ensure that systems access is removed within 24 hours of employment ending, as required by Section PS-4 of the Security Standard. One of five employees (20%) with systems access whose employment by Natural History ended during fiscal year 2019 did not have their systems access removed within 24 hours of employment ending.
- Natural History does not have a process in place for an annual review of systems access, as required by the Security Standard, Section AC-2.
- Natural History has not updated access control policies and procedures since 2017, which is not in compliance with Section AC-1 of the Security Standard requiring an annual update and review.

Inadequate access controls can result in improper or unnecessary access to sensitive systems, which can lead to a breach in data security. Natural History's limited IT personnel contributes to the internal control weaknesses identified. Natural History should devote necessary time and resources to

review and update access policies and procedures annually, implement an annual access review, and improve access controls to ensure a timely access termination process.

Develop a Process for Obtaining and Reviewing Audit Logs

ISS Control Area: Audit Logging

Natural History does not implement certain audit logging and monitoring safeguards for mission-essential sensitive systems in accordance with the Security Standard. We communicated three control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard requires audit logging and monitoring controls to protect the confidentiality, integrity, and availability of sensitive and mission-critical data. Due in part to limited personnel resources, Natural History was not able to implement the necessary safeguards described in the FOIAE document and comply with the Security Standard.

Natural History should dedicate the necessary resources to implement the security controls discussed in the communication marked FOIAE in accordance with the Security Standard. Implementing corrective action will help maintain the confidentiality, integrity, and availability of Natural History's sensitive and mission-critical data.

Improve Risk Management and Contingency Planning

ISS Control Area: Risk Management and Contingency Planning

Natural History is not properly maintaining IT risk management and contingency planning documentation in accordance with the Security Standard. A review of Natural History's IT risk management and contingency planning controls identified the following weaknesses:

- Natural History was unable to provide documentation to support IT risk assessments for sensitive systems as required in the Security Standard, Section 6.2.
- Natural History was unable to provide an annual self-assessment of sensitive system IT risk assessments to determine their continued validity as required in the Security Standard, Section 6.2.
- Natural History was unable to provide a current BIA as required in the Security Standard, Section 3.2.
- Natural History was unable to provide a DRP as required in the Security Standard, Section CP-1-COV-1.
- Natural History is not performing an annual exercise of the DRP components of the contingency plan as required in the Security Standard, Section CP-1-COV-1.

Natural History has an agreement with VITA to provide the following deliverables: BIA, system security plan (to include risk assessments and risk treatment plans), and enhanced security services (to include penetration testing, vulnerability assessments, and incident response planning). However, Natural History relies upon the provider to complete these services and does not retain or review deliverables upon their completion to ensure validity.

The Security Standard, Section CP-1-COV-1, requires that agencies use their BIA and risk assessments to develop IT disaster components of the agency contingency plan which identify each IT system that is necessary to recover agency business functions or dependent business functions and the RTO and RPO for each. It also requires an annual exercise of DRP components to assess their adequacy and effectiveness. Natural History's lack of understanding of Security Standard requirements related to IT risk management and contingency planning, along with limited personnel and IT resources contributed to the identified weaknesses above.

Natural History's current approach to IT risk management and contingency planning increases the risk that it will not identify and mitigate existing vulnerabilities, which could lead to delays in restoring systems that support mission-critical business functions in the event of an emergency or disaster. Natural History should develop a process to ensure that it retains and updates deliverables completed by the provider in accordance with the Security Standard. Maintaining current IT risk management and contingency planning documentation will decrease the data security risk for the sensitive systems and improve the overall security of the control environment.

Improve Security Awareness Training Program

ISS Control Area: Security Awareness Training

Natural History is not adequately administering, monitoring, or enforcing annual security awareness training for all information system users. During calendar year 2019, only 31 percent of Natural History employees completed security awareness training. Further, Natural History is not providing consistent security awareness training, as two different training platforms are used to administer training. Section AT-2 of the Security Standard requires organizations to provide basic security awareness training to information system users as part of initial new hire training, when required by information system changes, and annually or more often as necessary thereafter. Additionally, Section AT-4 requires organizations to document and monitor individuals' completion of security awareness training.

Natural History has not allocated appropriate resources to ISS, which has resulted in an inadequate process of administering and monitoring training to ensure completion. Natural History should consider using one training platform to provide a consistent security awareness training program to all employees. Without management's enforcement and emphasis on the importance of security awareness training, information system users may lack the knowledge to identify and respond to security threats that could compromise sensitive systems and data. Natural History should improve upon its monitoring process to ensure that all information system users complete security awareness training as required by the Security Standard.

Improve Oversight of Third-Party Providers

ISS Control Area: Third-Party Provider Oversight

Natural History uses a provider to provide and host a system that supports their mission-critical business functions. Natural History does not have a process in place to gain assurance that the provider has adequate security controls to protect sensitive data. Natural History's current MOU with the provider does not include security requirements in accordance with the Hosted Environment Security Standard. Additionally, Natural History does not perform the following oversight functions as required by Section SA-9-COV-3 of the Hosted Environment Security Standard:

- Perform an annual security audit of the environment or review the annual audit report of the environment conducted by an independent, third-party audit firm on an annual basis.
- Perform a monthly review of activity logs related to the operation of the service.
- Receive vulnerability scans of the operating system and supporting software from the provider at least once every 90-days.

Section 1.1 of the Hosted Environment Security Standard states that the agency head is accountable for maintaining and enforcing compliance with this standard through documented agreements with providers and oversight of the services provided. Without a process to gain assurance over providers' operating controls, Natural History cannot validate that providers have effective security controls for protecting sensitive data, which puts Natural History's, and therefore the Commonwealth's, information at risk. Natural History's lack of IT personnel resources, and corresponding constraints on their time, is a primary contributor for not having a process to gain assurance over providers.

Management should consider developing and implementing a process to maintain oversight of providers. Given the limited IT resources, Natural History may also consider using ECOS provided by VITA. ECOS provides oversight and gains assurance over providers' operating controls. Developing and implementing an oversight process will provide Natural History with assurance over the confidentiality, availability, and integrity of systems which support mission-critical business functions.



Staci A. Henshaw, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

October 4, 2021

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

We have audited the information systems security (ISS) of 19 Commonwealth agencies and are pleased to submit our report entitled *Cycled Agency Information Systems Security Review*. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit evaluated ISS areas against the Commonwealth's Security Standard and the Hosted Environment Security Standard. We reviewed the agency's policies and procedures and the structure of the ISS operations. We performed procedures over access control policies, annual access reviews, and access termination. We tested the audit and accountability policy and the controls that support the policy. We reviewed information system risk assessments, business impact analyses, ISS audits, third-party service provider agreements including the enterprise cloud oversight services (ECOS) service, and continuity of operation plans. We reviewed the security awareness training policy, the training topics covered, and users' training completion. We tested each agency's third-party oversight documentation and procurement risk assessments.

Conclusion

Our audit found several internal control deficiencies related to ISS. These deficiencies included:

- Inadequate policies and procedures for ten out of 19 agencies (53%)
- Insufficient IT governance controls for five out of 19 agencies (26%)
- Insufficient access controls for 14 out of 19 agencies (74%)

- Insufficient audit logging controls for 12 out of 19 agencies (63%)
- Insufficient risk management and contingency planning controls for 16 out of 19 agencies (84%)
- Insufficient security awareness training controls for seven out of 19 agencies (37%)
- Insufficient third-party provider oversight controls for four out of 19 agencies (21%)
- Noncompliance with laws and regulations governing information system controls for 17 out of 19 agencies (89%)

Exit Conference and Report Distribution

We discussed this report with management of each agency. Management's response to the findings identified in our audit is included in the section titled "Agency Response." We did not audit management's response and, accordingly, we express no opinion on it.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

DLR/vks



COMMONWEALTH of VIRGINIA

Department of Agriculture and Consumer Services

PO Box 1163, Richmond, Virginia 23218

www.vdacs.virginia.gov

Joseph W. Guthrie
Commissioner

February 8, 2022

Ms. Staci Henshaw
Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

Thank you for the opportunity to review the draft APA Information System Security Review for FY 2019 report. We appreciate the opportunity to examine of the Virginia Department of Agriculture and Consumer Services' information technology security program, and we are making continuous improvements to the security environment.

We appreciate the assistance of your staff and look forward to working with you again.

Sincerely,

A handwritten signature in cursive script that reads "Joseph W. Guthrie".

Joseph W. Guthrie
Commissioner

-Equal Opportunity Employer-



COMMONWEALTH of VIRGINIA
DEPARTMENT OF CONSERVATION AND RECREATION

October 19, 2021

Ms. Staci A. Henshaw, CPA
The Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

The Department of Conservation and Recreation (DCR) appreciates the opportunity to respond to the Auditor of Public Accounts (APA) Information System Security Review for FY2019.

While DCR concurs with the six (6) findings contained in this FY2019 report from 15 months ago, DCR has already implemented corrective actions as detailed below.

Review and Update Policies and Procedures

The DCR has reviewed and updated its information security policies and has implemented a process to review them on an annual basis, as stated in DCR's IT Security Policy No. 427.

Improve Access Controls

System access for both sensitive systems is now being reviewed on an annual basis, as required by the Security Standard, Section AC-2. The documentation of these reviews is being retained. The DCR has developed a detailed procedures document for system access requests for each sensitive system, as required by the Security Standard, Section AC-1. The procedures include a system access request form and request approval process.

The DCR strives to disable information system access within 24 hours of employment termination, as required by Security Standard, Section PS-4. The agency currently has an off-boarding process that includes the disablement of employee access.

Improve Audit Log Controls

The DCR was reviewing audit logs on a quarterly basis. As a result of the audit recommendation, the Agency is now reviewing the audit logs every 30 days and retaining a record of these reviews.

Review and Update System Risk Assessments

The DCR was conducting risk assessments for sensitive systems every 3 years, but was not reviewing and updating the risk assessments each year. The Agency has revised its process to review and update the risk assessments each year, as required in the Security Standard, Section 6.2. The Agency is also retaining a record of these reviews.

600 East Main Street, 24th Floor | Richmond, Virginia 23219 | 804-786-6124

*State Parks • Soil and Water Conservation • Outdoor Recreation Planning
Natural Heritage • Dam Safety and Floodplain Management • Land Conservation*

Perform Disaster Recovery Testing

The DCR has an IT disaster recovery plan, and its normal operations include backup and restoration processes throughout the year. The DCR has updated the IT disaster recovery plan to include annual testing of the plan, as required by the Security Standard Section CP-1-COV-1, and will begin testing this year.

Improve Security Awareness Training Program

The DCR provides security awareness training annually to all employees, as required by the Security Standard Section AT-2. As a result, in 2020 all employees did complete the training.

I would personally like to state our appreciation for the level of professionalism and guidance provided by you and your staff throughout this engagement. Please contact me should you have any questions or concerns.

Sincerely,



Clyde Cristman
DCR Director



COMMONWEALTH of VIRGINIA

Department of Criminal Justice Services

Shannon Dion
Director

Megan Peterson
Chief Deputy Director

Washington Building
1100 Bank Street
Richmond, Virginia 23219
(804) 786-4000
www.dcjs.virginia.gov

December 13, 2021

Mrs. Staci Henshaw
Auditor of Public Accounts
101 North 14th Street
Richmond, VA 23219

Re: DCJS Response to APA Information Systems Security Audit Report

Dear Mrs. Henshaw,

We appreciate the opportunity to respond to the APA Information Systems Security report. The Department is in agreement with your findings and has made great strides to improve our IT Security Governance in recent months. In August 2021, DCJS added a full-time Information Security Officer (ISO) position to its staff. As required by the Commonwealth of Virginia, Information Technology Resource Management, Information Security Standard (SEC501), Section 2.4.1, this position reports directly to the Agency Director. The ISO's primary function is to manage the agency's Information System Security structure in accordance with SEC501, which includes implementation, development, and remediation efforts. This includes all SEC501 required policies and procedures. The position, in partnership with the Computer Services team, is also in the process of developing an agency IT Disaster Recovery Plan.

The department has many legacy systems that could not be updated to meet the required ISS controls due to aging technology. As a result, we are in the process of replacing these legacy systems with more current technology. These new solutions will incorporate and comply with SEC501 system security requirements, including logical access controls and audit logging. The plan is to have these systems replaced within the next three years following the state's procurement procedures.

Sincerely,

Shannon Dion



COMMONWEALTH of VIRGINIA DEPARTMENT OF ELECTIONS

Christopher E. "Chris" Piper
Commissioner

March 11, 2022

Department of Elections 3 of 7

Agency	Policies and Procedures	IT Governance	Access Control	Audit Logging	Risk Management and Contingency Planning	Security Awareness Training	Third-Party Provider Oversight
Conservation and Recreation	X	✓	X	X	X ²	X	✓
Criminal Justice	X	X	X	X	X	✓	✓
ELECT	X	✓	X	X	X	✓	✓

Department of Elections

Develop and Implement Policies and Procedures

ISS Control Area: Policies and Procedures

ELECT does not have properly executed policies and procedures in place to comply with the Security Standard. The Security Standard, Section 2.4.2, requires that an information security program be maintained, is adequate to protect IT systems, and is effectively communicated throughout the organization. ELECT has developed draft policies that are going through the approval process; however, all necessary policies and procedures have not been approved and implemented as required in the Security Standard, Sections AC-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, and SI-1.

Limited IT personnel and resources available to ELECT along with recent turnover in key information security positions contributed to the identified weaknesses. A lack of policies and procedures surrounding information system security may result in insufficient or inappropriate processes and leaves the agency at risk for improper system usage due to lack of formal guidance. ELECT should develop, approve, and implement policies and procedures surrounding information system security to ensure that the agency's information system processes align with the requirements of the Security Standard.

Response:

ELECT in 2019 began a holistic review of our information security governance framework and through the first half of 2020, worked with experts in information security and information technology to create policies and procedures to comply with COV525. This governance effort has now evolved to implementation of this framework that continues. In July and August 2021, a governance audit conducted by Impact Makers

confirmed and ascertained ELECT's level of compliance with developing and implementing InfoSec policies including AC-1, AT-1, AP-3, AU-1, CA-1, CM-1, IA-1, IR-1, PS-4, PS-6, RA-2, RM-1, SA-15, SI-1, SI-2, SI-11, SI-12.

Improve Access Controls

ISS Control Area: Access Control

ELECT does not have appropriate internal controls in place to ensure that access to their systems is appropriate and complies with the requirements of the Security Standard. Specifically, ELECT has weaknesses in the following areas:

- ELECT does not consistently require confirmation of the account request and approval by the IT system user's supervisor and approval by the data owner or designee, or the ISO to establish accounts on all sensitive systems, as required by the Security Standard Section AC-2-COV.
- ELECT does not have an adequate process in place for reviewing and confirming ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization as required by the Security Standard Section PS-5.
- For eight of the ten (80%) employees sampled ELECT could not provide documentation to support the removal of systems access within 24 hours of employment termination, as required by the Security Standard, Section PS-4.
- ELECT does not have an adequate process in place for an annual review of systems access, as required by the Security Standard, Section AC-2.

Inadequate access controls could result in improper or unnecessary access to sensitive systems, which could lead to a breach in data security. Limited IT resources and personnel available to ELECT combined with recent turnover in key information security positions has contributed to the lack of appropriate access controls. ELECT should improve their access processes to ensure that they align with the Security Standard to ensure consistent and appropriate account management and ensure the protection of sensitive information.

Response:

ELECT's Security Division placed as their top priority for 2022 the effort to lead ELECT divisions in reviewing ELECT systems, updating the list of sensitive systems and the process to assign, train and implement review processes for and by data owners, custodians, system owners and administrators.

Improve Audit Logging and Review Process

ISS Control Area: Audit Logging

ELECT does not implement certain audit logging and monitoring safeguards for a sensitive system in accordance with the Security Standard. We communicated three internal control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard requires audit logging and monitoring controls to protect the confidentiality, integrity, and availability of sensitive and mission-critical data. Due in part to limited resources, ELECT was not able to implement the necessary safeguards described in the FOIAE document and comply with the Security Standard.

ELECT should dedicate the necessary resources to implement the security controls discussed in the communication marked FOIA Exempt in accordance with the Security Standard. This will help maintain the confidentiality, integrity, and availability of ELECT's sensitive and mission-critical data.

Response:

ELECT is currently engaged in a procurement process to identify, obtain and implement a voter registration system with appropriate logging parameters that will fulfill COV requirements for audit logging to enable appropriate monitoring of systems with sensitive information essential for ELECT to ensure remains confidential, integral and available.

Perform Disaster Recover Testing

ISS Control Area: *Risk Management and Contingency Planning*

ELECT has not performed an annual exercise of their IT DRP, as required by the Security Standard. Section CP-1-COV-1 of the Security Standard requires that organizations perform an annual exercise of IT disaster recovery components to assess their adequacy and effectiveness.

ELECT was part of a large disaster recovery exercise through VITA, which was performed by an external vendor. The external vendor was not able to complete testing for ELECT due to problems with the infrastructure setup. ELECT communicated with VITA to correct the issue, however, the infrastructure correction was not performed in time for a re-test, so testing was not performed.

Without a well-tested disaster recovery plan in place, ELECT may not be able to restore the systems that support mission-essential business functions in a timely manner in the event of an emergency or disaster. ELECT should ensure proper communication with VITA to ensure that their infrastructure is appropriately configured for disaster recovery testing and should perform an annual test of disaster recovery components to assess their adequacy and effectiveness.

Response:

ELECT Security placed as their second highest priority for 2022 to organize and manage the agency's revisions to and implementation of an ELECT Disaster Recovery plan that will be primarily implemented by ELECT's Information Services division with the goal of accomplishing this project by the end of Q2 of 2022.



COMMONWEALTH OF VIRGINIA

Virginia Department of Energy
Washington Building / 8th Floor
1100 Bank Street
Richmond, Virginia 23219-3638
(804) 692-3200 FAX (804) 692-3237
www.energy.virginia.gov

October 12, 2021

Stacy Henshaw, Auditor of Public Accounts
Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

RE: Response to Results Letter of ISS Audit Report Review

Dear Ms. Henshaw:

We concur with the findings noted in the letter. The Agency has implemented a Corrective Action Plan for each of the items noted.

- Updated Policies and Procedures have been developed.
- Access control procedures have been improved by improved coordination with HR to coordinate termination of access in a timely manner.
- Audit Logs are reviewed regularly and the review is documented.

We appreciate the review and will make the required changes and improvements in our internal controls.

Sincerely,

John W. Warren
Director

EQUAL OPPORTUNITY EMPLOYER
TDD (800) 828-1120 --- Virginia Relay Center



COMMONWEALTH of VIRGINIA

Department of Forestry

900 Natural Resources Drive, Suite 800 • Charlottesville, Virginia 22903
(434) 977-6555 • Fax: (434) 296-2369 • www.dof.virginia.gov

December 13, 2021

Dear Ms. Henshaw:

Below is our response to the audit findings of August 27, 2020.

- Forestry has not reviewed and updated its information security policies and procedures since 2011, which does comply with the annual review and update requirement in the Security Standard, Sections AC-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, and SI-1.

Agency Response: The agencies new IT team has started the review process and has determined that additional contract staffing will be required to complete the task. The agency is in the process of determining a source of expertise to contract with to complete the development of an agency information security plan.

- Forestry does not have an ISO that is independent from IT operations, as required in the Security Standard, Section 2.4.1.

Agency Response: Forestry is a small state agency, does not currently have sufficient resources to hire a dedicated ISO position. Forestry has requested funds in the upcoming budget, FY22-24, to hire a full-time position to carry-out this responsibility.

- Forestry's current access termination process is not adequate to ensure that systems access is removed within 24 hours of termination, as required by Section PS-4 of the Security Standard. In a sample of five employees who terminated from Forestry in fiscal year 2019, four employees (80%) did not have their systems access removed within 24 hours of termination.

Agency Response: Forestry information technology management is working with agency HR staff to document and streamline the communication of agency personnel both on-boarding and off-boarding to ensure IT adds and removes staff system access in a timely manner.

- Forestry was unable to provide documentation to support an annual review of systems access, as required by the Security Standard, Section AC-2.

VDOF APA audit response 2020.docx

Agency Response: Forestry information technology section has implemented a new process of annual review of agency systems access for all staff.

- We communicated these specific control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Agency Response: Forestry's legacy information system, [REDACTED] relies on older technologies and does not have expanded audit log capabilities. We are in the process of determining a replacement for [REDACTED] that will allow for the collection and review audit logs among other enhancements to our current capabilities. Determination of the solution will be in early calendar year 2022.

- Forestry was unable to provide documentation to support IT risk assessments for sensitive systems as required in the Security Standard Section 6.2.

Agency Response: Forestry has partnered with Commonwealth Information Security Services to perform IT risk assessments on all sensitive systems.

- Forestry was unable to provide an annual self-assessment of sensitive system IT risk assessments to determine their continued validity as required in the Security Standard Section 6.2.

Agency Response: Forestry has partnered with Commonwealth Information Security Services to perform IT risk assessments on all sensitive systems as well as annual review of all RAs.

- Forestry was unable to provide a BIA as required in the Security Standard Section 3.2.

Agency Response: Forestry has partnered with Commonwealth Information Security Services to perform Business Impact Analysis on all sensitive systems.

- Forestry does not maintain a current continuity of operations and IT disaster recovery plan (Contingency Plan). The provided contingency plan was last updated in 2015 and included reference to retired information systems and other outdated information.

Agency Response: Forestry has updated the disaster recovery plan for their [REDACTED] system. The solution is a backup server for the [REDACTED] application located off-sight at our application host [REDACTED]

Note: Certain information, marked with a black box, was redacted from management's response because it being Freedom of Information Act Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms.

- Forestry is not performing an annual exercise of the IT disaster recovery components of the contingency plan as required in the Security Standard Section CP1-COV-1.

Agency Response: Forestry has completed annual exercise of IT disaster recovery on [REDACTED] system in Oct 2021 and plans to do so annually.

- Forestry is not adequately administering, monitoring, or enforcing annual security awareness training for all information system users. Forestry's security awareness training program has not been updated since 2009 and is not being completed by all users as required by the Security Standard.

Agency Response: Forestry has partnered with [REDACTED] security platform to implement new security awareness training program. Annual security awareness training for 2021 is underway and expect to be completed by end of the month.

- Perform an annual security audit of the environment or review the annual audit report of the environment conducted by an independent, third-party audit firm on an annual basis.

Agency Response: Forestry is implementing a process to request and review annual audit documentation from third-party vendors on all hosted solutions.

- Perform a monthly review of activity logs related to the operation of the service.

Agency Response: Forestry is implementing a process to request and review activity logs from third-party vendors on all hosted solutions.

- Receive vulnerability scans of the operating system and supporting software from the provider at least once every 90-days.

Agency Response: Forestry is implementing process to request and review vulnerability scans at least once every 90 days from third-party vendors on all hosted solutions.

 12/13/2021
VDOF, Chief of Administration

Note: Certain information, marked with a black box, was redacted from management's response because it being Freedom of Information Act Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms.



COMMONWEALTH of VIRGINIA

David E. Brown, D.C.
Director

Department of Health Professions

Perimeter Center
9960 Mayland Drive, Suite 300
Henrico, Virginia 23233-1463

www.dhp.virginia.gov
TEL (804) 367-4400
FAX (804) 527-4475

October 14, 2021

Ms. Staci A. Henshaw, CPA
The Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw,

The Department of Health Professions (DHP) appreciates the opportunity to respond to the results of the Information Systems Security (ISS) Audit performed by your staff for the fiscal year ending June 30, 2019. Your staff was a pleasure to work with during the audit. They were thorough, knowledgeable, and kept communications open and engaged throughout the audit.

DHP agrees with the audit team's two findings as written and would like to provide the below updates for the findings:

Improve Communication of Access Controls

The Department of Health Professions (DHP) has made improvements and communicated the improved process for employee access terminations to both DHP supervisors and Human Resources to ensure that access is removed in a timely manner. In order to ensure DHP's Supervisor understood the responsibilities for providing the employee employment status information properly, DHP IT Security Policy and Program Section B, 76-70.05b, AC-1 Access Control Policy and Procedures, was revised to address the criteria for disabling an employee or contractor's account. DHP's Chief Operating Officer communicated the updated termination process to supervisors through several emails during FY-2021. Additionally, employees who go on VSDP will be communicated to the Information Security team to monitor those accounts and disable when necessary. These communications have resulted in a better understanding between DHP Supervisors and Human Resources Personnel regarding the responsibility for informing DHP's IT Security Unit of terminations on a timely basis. During DHP's recent FY-2021

Board of Audiology & Speech-Language Pathology – Board of Counseling – Board of Dentistry – Board of Funeral Directors & Embalmers
Board of Long-Term Care Administrators – Board of Medicine – Board of Nursing – Board of Optometry – Board of Pharmacy
Board of Physical Therapy – Board of Psychology – Board of Social Work – Board of Veterinary Medicine
Board of Health Professions

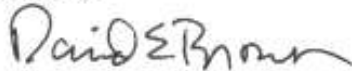
ARMICS review, the testing of users' terminations noted minimal response time for supervisors to notify IT Security of employee terminations.

Perform Disaster Recovery Testing

The Department of Health Professions (DHP) Disaster Recovery Team met several times during FY 2021 and identified the applications to restore that support mission-critical business functions in a timely manner in the event of an emergency or disaster. The Disaster Recovery Team developed a process for annual testing of the IT disaster recovery plan to ensure the timely restoration of mission essential functions in the event of a disaster. The Disaster Recovery Team completed the testing of DHP's mission critical applications and documented the results in the January 22, 2021, Disaster Recovery Testing document. The Disaster Recovery Team has initiated the IT Disaster Recovery Plan testing for FY-2022 and are currently documenting the timely restoration of DHP's mission essential functions.

DHP is committed to excellence and continuous improvement, so we welcome the opportunity to work with your staff to obtain additional guidance on best practices and internal controls for our information systems. Again, thank you and your staff for the high level of professionalism and cooperation during this audit.

Sincerely,



David E. Brown, D.C.
Director

cc: Lisa Russell Hahn, Chief Operating Officer
Robert Jenkins, Director, Technology & Business Services
Chris Moore, Finance and Budget Director



Ralph S. Northam
Governor

R. Brian Ball
Secretary of
Commerce and Trade

COMMONWEALTH of VIRGINIA

DEPARTMENT OF HOUSING AND COMMUNITY DEVELOPMENT

Erik C. Johnston
Director

The Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Mrs. Henshaw:

In connection with the audit of information systems security (ISS) at the Department of Housing and Community Development (DHCD) for fiscal year ended June 30, 2019, we offer the responses below to the audit concerns that were raised.

ISS Control Area: IT Governance

Housing does not have adequate controls over IT governance, as required by the Security Standard. Specifically, Housing has weaknesses in the following areas:

- Housing does not separate the roles of the ISO and the CIO as required by the Security Standard, Section 2.4.1, which states that the ISO must not simultaneously serve the function of a CIO.
- Housing does not retain the memorandum of understanding (MOU) between Housing and VITA, as required by the Security Standard, Section 1.3, which states that the agency shall maintain documentation regarding specific roles and responsibilities relating to information security.

Agency Response: DHCD concurs and has updated policies and procedures to ensure that a COV Information Security Policy & Standard Exception request is timely submitted to VITA. Additionally, DHCD has obtained and will continue to retain an active memorandum of understanding (MOU) between DHCD and VITA, as required by the Security Standard, Section 1.3.

ISS Control Area: Access Control

Housing does not have adequate internal controls in place to ensure that access termination complies with the requirements of the Security Standard. In a sample of three



Virginia Department of Housing and Community Development | Partners for Better Communities
Main Street Centre | 600 East Main Street, Suite 300 Richmond, VA 23219
www.dhcd.virginia.gov | Phone (804) 371-7000 | Fax (804) 371-7090 | Virginia Relay 7-1-1

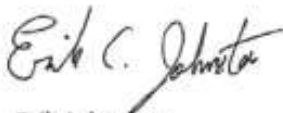
employees who terminated from Housing in fiscal year 2019, one employee (33%) did not have their systems access removed within 24 hours of termination, as required by Section PS-4 of the Security Standard. Housing submitted the request to remove system access five days following the employee's termination.

Agency Response: DHCD concurs and have updated policies and procedures to ensure that employee system access for terminated employees is removed within 24 hours.

DHCD agrees with the weaknesses outlined in the information systems security (ISS) audit report and has taken corrective actions to address these areas.

DHCD appreciates your partnership and is committed to continual improvement.

Sincerely,



Erik Johnston
DHCD Director



Virginia Department of Housing and Community Development | Partners for Better Communities
Main Street Centre | 600 East Main Street, Suite 300 Richmond, VA 23219
www.dhcd.virginia.gov | Phone (804) 371-7000 | Fax (804) 371-7090 | Virginia Relay 7-1-1

October 20, 2021

The Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

This letter is being provided in connection with your report on the fiscal year 2019 audit of the information systems security of the Department of Juvenile Justice (DJJ). We confirm we are responsible for establishing appropriate information security policies and procedures, information technology (IT) governance, access control, audit logging, risk management and contingency planning, security awareness training, and third-party provider oversight.

We appreciate the recommendations you made and, in the interim, have been working diligently to address them. The following is a summary of where we are now.

1. Update Policies and Procedures

On September 2, 2020, DJJ released a comprehensive overhaul of the DJJ information security program. These overhauled program documents are intended to address this issue and to better align the Department's information security program with the Commonwealth's policies and standards. These documents are also intended to provide a foundation upon which data and system owners can develop appropriate procedures to ensure the security of the sensitive information we handle.

2. Improve Access Controls

Since September of 2020, DJJ has been reviewing our business processes, data sets, and associated systems with the purpose of improving our understanding of the connections between our business processes and our information security responsibilities. We are developing improved guidance for system owners to help them understand their access control responsibilities, and to improve documentation of their regular reviews of authorized users. DJJ is also in the requirements gathering stage of a project to develop a human resources information system that will include components to facilitate the on-boarding, internal moving between positions and off-boarding of employees.

3. Improve Process for Reviewing Audit Logs

Since September of 2020, DJJ has been reviewing our business processes, data sets, and associated systems with the purpose of improving our understanding of the connections between our business processes and our information security responsibilities. We are developing improved guidance for system owners to help them understand their audit log review responsibilities, and to improve documentation of their quarterly reviews of system audit logs.

4. Update Risk Assessment and Contingency Planning

DJJ is working with the Virginia Information Technologies Agency (VITA) Centralized Security Service to review, revise, and update the Department's business impact analysis, risk assessments and disaster recovery plans. The DJJ information security team also now includes the DJJ risk manager as a backup ISO to improve coordination between the Department's contingency plans and business continuity plan. DJJ also participated in the 2021 Commonwealth Disaster Recovery Exercise to provide documented testing of the Department's contingency plans.

5. Perform IT Security Audits

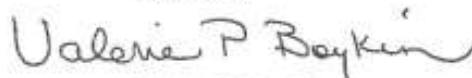
DJJ is working with VITA's Centralized IT Security Audit Service to perform audits of the Department's sensitive systems, and document these audits, any associated findings, and to develop corrective action plans to address the findings.

6. Perform Annual Security Awareness Training

In 2020, DJJ restarted the Department's mandatory end user information security awareness training program for all employees who access sensitive DJJ systems or handle sensitive departmental information. In 2021, we expanded this mandatory security awareness training to include the Department's external business partners who access sensitive DJJ systems or handle sensitive departmental information. The information security team and the Department's training and organizational development team are also working within the Virginia Learning Center to develop and implement the annual required role-based information security awareness training to ensure that system owners, data owners, system administrators, and senior leadership are complying with the additional training responsibilities associated with their assigned positions.

Please feel free to contact the Department if you have additional questions or concerns.

Sincerely,

A handwritten signature in cursive script that reads "Valerie P. Boykin".

Valerie P. Boykin



COMMONWEALTH of VIRGINIA
DEPARTMENT OF LABOR AND INDUSTRY

C. Ray Davenport
COMMISSIONER

Main Street Centre
600 East Main Street, Suite 207
Richmond, Virginia 23219
PHONE (804) 371-2327
FAX (804) 371-8524

October 19, 2021

Ms. Staci Henshaw
Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

Thank you for the opportunity to respond to the Information Security Systems Audit for the Department of Labor and Industry (DOLI). The Department concurs with the findings and will ensure corrective action is implemented in a timely manner.

We appreciate the courtesy and professionalism of your staff during the review.

Sincerely,

A handwritten signature in blue ink that reads "C. Ray Davenport".

C. Ray Davenport
Commissioner



COMMONWEALTH of VIRGINIA

MG TIMOTHY P. WILLIAMS
THE ADJUTANT GENERAL

DEPARTMENT OF MILITARY AFFAIRS
OFFICE OF THE ADJUTANT GENERAL
VIRGINIA NATIONAL GUARD

JOINT FORCE HEADQUARTERS
8000 JEFFERSON DAVIS HWY
BUILDING 430
RICHMOND, VA 23297

October 20, 2021

The Auditor of Public Accounts
Attn: Staci Henshaw
PO Box 1295
Richmond, VA 23218

Dear Ms. Henshaw,

Please accept this as the Agency Response to the draft findings listed in your 8 October 2021 letter as a result of the Information System Security Review for Fiscal Year 2019.

The Department of Military Affairs appreciates the level of detail in this year's audit and concurs with the draft report. We are proud of the work we do supporting the Virginia National Guard and we recognize there are areas that need attention. We will diligently work to correct these weaknesses in the coming months.

We will file the required corrective action plan with the State Comptroller within 30 days of receipt of our official APA audit report. We thank you and your staff for your review and the assistance you have provided us. Please contact me at donald.l.unmussig.nfg@mail.mil or 434-298-6385 for the final results. I will provide those to the Agency Head through a special briefing.

Sincerely,

Donald L. Unmussig
CFO, VA Department of Military Affairs



COMMONWEALTH of VIRGINIA

Department of Professional and Occupational Regulation

Glenn A. Youngkin
Governor

G. Bryan Slater
Secretary of Labor

Demetrios J. Melis
Director

January 25, 2022

Staci A. Henshaw, CPA
Auditor of Public Accounts
PO Box 1295
Richmond, VA 23218

Re: Agency Response to the 2019 Information Systems Security review

Dear Ms. Henshaw:

Thank you for the opportunity to review and comment on the Information Systems Security review findings. The Department is committed to maintaining strong systems security. As the new Director, I am in the process of recruiting for the vacant IT Director position and hope to have it filled in the very near future. I have also implemented some immediate stop gap efforts to better structure our IT operations.

In talking with agency staff who were present during the audit, they commented on your staff's courteous and fair demeanor and understanding of the additional workload placed on our IT staff due to vacancies. For that we are very much appreciative.

The agency concurs with the findings and recommendations made in the review. Two of the four items identified have been resolved and verified by the APA during our 2020 ICQ review. The Department is taking corrective actions to resolve the other two items.

Sincerely,

Demetrios J. Melis
Director



Ralph S. Northam
Governor

COMMONWEALTH of VIRGINIA

R. Brian Ball
Secretary of Commerce & Trade

Department of Small Business and Supplier Diversity

Matthew James
Director

October 19, 2021

Via Electronic Mail
Staci A. Henshaw, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Ms. Henshaw:

The Department of Small Business and Supplier Diversity's (SBSD) response to the results of the APA's Information System Security Review for 2019 (received via e-mail on October 11, 2021) follows.

Result – Improve Audit Log Controls

Small Business and Supplier Diversity does not have adequate internal controls over the audit logging process, as required by Hosted Environment Security Standard. (Excerpt of Finding)

Agency Response

Small Business and Supplier Diversity is working on the corrective action to Improve Audit Log Controls. SBSD does have paper trail logs and new relic alert events and are working to generate a report for this data.

For AU-2 - Audit Events - Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes are captured in paper trail logs

For AU-6 Audit Review, Analysis and Reporting - Reviews and analyses of information system audit records are performed at least once a week for indications of inappropriate or unusual activity and any findings are reported to designated organization officials.

Result – Perform Disaster Recovery Testing

Small Business and Supplier Diversity is not properly testing their IT DRP as required by the Security Standard. Section CP-1-COV-1 of the Security Standard requires that agencies perform an annual exercise of IT disaster recovery components to assess their adequacy and effectiveness. Small Business and Supplier Diversity did not have a clear understanding of the services provided by VITA and believed their VITA services included IT DRP testing. (Excerpt of Finding)

Agency Response

Small Business and Supplier Diversity thought that Disaster Recovery Services were included in the services provided by VITA. Once it was determined Disaster Recovery Services were not included, SBSD signed up for Disaster Recovery Services with VITA in August of 2020.

In August of 2021, SBSD participated in the Disaster Recovery Exercise. The exercise included the following:

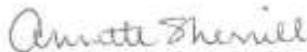
Our 2021 DR Exercise included.

1. Exercising Standard Operating Procedure – Emergency Communication Notification
2. Mainframe Services – Bringing up mainframe services at DR location (Colorado Springs)
3. Exercise COV Agencies readiness connecting to DR IT protected environments
4. Exercise DR infrastructure required for COV agencies to test their mainframe applications
5. Provide emergency management basic training to crisis situation
6. Exercise COV agencies reactive response to approaching disaster situation and once it strikes
7. Exercise decision process when COV agencies move from production environment to DR environment
8. Identify gaps within COV agencies DR documentation
9. Identify gaps within Continuity Service process supporting COV

The DR Exercise Activity Tracker is attached.

The agency will continue to participate in the annual Disaster Recovery testing with VITA.

Sincerely,



Annette Sherrill
Director of Administration

cc. Matthew James, Director



March 21, 2022

VIDC RESPONSE TO APA AUDIT FINDINGS AND RECOMMENDATIONS

During the Virginia Indigent Defense Commission's (VIDC) audit during 2019, the Auditor of Public Accounts noted four ISS Control areas named below:

- Strengthen Policies and Procedures
- Improve Controls over Access Removal for terminated Employees
- Risk Management and Contingency Planning
 - Ensures Completion of Validity of Risk Assessments
 - Perform Disaster Recovery Testing, and
- Improve Oversight of Third-Party Providers.

Following are the Virginia Indigent Defense Commission's responses to those comments:

Strengthen Policies and Procedures

As noted by the APA this is a result of lack of IT personnel. VIDC contracted with VITA for ISO services in 2019. That contract contemplated the ISO addressing this need or, at the very least, aid VIDC in addressing this need. The VITA ISO has not provided any of those contracted services. VIDC is currently recruiting for two additional staff. If staffing is found this will be a duty assigned to one of the additional staff. VIDC notes that finding qualified IT staff during the current recruitment climate is challenging especially with the salary funding provided.

Improve Controls over Access Removal for terminated Employees

New processes have been undertaken since the 2019 audit as well as the employee responsible for the noted concerns is no longer employed with the VIDC. Replacement staff have proven more accurate. Further, VITA conducted an audit during a somewhat overlapping time period and specifically looked at this ISS control areas and noted NO concerns.



Risk Management and Contingency Planning

Ensures Completion of Validity of Risk Assessments

Much Like the Policies and Procedures VIDC contracted for, expected, but did not received VITA ISO assistant in this area. VIDC is currently recruiting for two additional staff and one will aid in addressing this ISS control. VIDC notes that finding qualified IT staff during the current recruitment climate is challenging especially with the salary funding provided.

Perform Disaster Recovery Testing

VIDC is currently recruiting for two additional staff that and one will aid in addressing this ISS control. VIDC notes that finding qualified IT staff during the current recruitment climate is challenging especially with the salary funding provided.

Improve Oversight of Third-Party Providers

VIDC will seek to add this requirement/mandate when VIDC engages or renews contracts with third party providers.

Sincerely,

David Johnson

Jamestown-Yorktown Foundation

P.O. Box 1607, Williamsburg, Virginia 23187-1607
(757) 253-4838 (757) 253-5299 Fax (757) 253-5110 TDD jymuseums.org

October 13, 2021

Auditor of Public Accounts
PO Box 1295
Richmond, VA 23218

Dear Mrs. Henshaw:

Thank you for the opportunity to comment on the Auditor of Public Accounts Information System Security Review.

Our staff continues to work to address the findings identified in the audit. As noted in the review, the Foundation's limited resources and staff are a contributing factor to the findings and limit our ability to address the identified weaknesses.

Since the conclusion of the audit, steps have been taken to improve access control, review risk assessments and provide security awareness training. We continue to work to meet the recommendations regarding monitoring audit logs, disaster recovery testing and oversight of third party providers. We are cognizant of the need to maintain a secure IT environment and we remain committed to addressing the weaknesses while maintaining our ability to meet other security requirements and operational needs.

I would like to commend your staff for their professionalism and consideration as we adjusted to the pandemic related complications of remote fieldwork, closed offices and staff furloughs. The cooperation from your staff was greatly appreciated.

As always, please know we appreciate your guidance and support.

Sincerely,



Christy S. Coleman

CSC/jlp

cc: The Honorable Kenneth R. Plum
Mr. Frank N. Stovall
Mrs. Jean L. Puckett

educating • interpreting • preserving • commemorating



An Agency of the
Commonwealth of Virginia

Accredited by the
American Alliance
of Museums

Kenneth R. Plum
Chairman

Janel D. Howell
Vice Chairman

Sue H. Gerdeman
Secretary

Dolores L. McQuinn
Treasurer

Christy S. Coleman
Executive Director

An Equal Opportunity
Employer/Affirmative Action
Organization



COMMONWEALTH OF VIRGINIA

Office of the State Inspector General

Michael C. Westfall, CPA
State Inspector General

P.O. Box 1151
Richmond, VA 23218

Telephone 804-625-3255
Fax 804-786-2341
www.osig.virginia.gov

October 15, 2021

David Rasnic, CPA, CISA
Audit Director, Higher Education Programs
Auditor of Public Accounts
101 N. 14th St, 8th Floor
Richmond, VA, 23219

Re: Disaster Recover Testing, ISS Control Area: Risk Management and Contingency Planning

Dear Mr. Rasnic,

The Office of the State Inspector General received your email indicating that OSIG was not adequately testing its IT Disaster Recovery Program during FY 2019; specifically, that OSIG was not performing dedicated disaster recovery testing due to a lack of understanding that normal restores are not sufficient to satisfy the requirements of the Security Standard.

OSIG accepts this finding and has mitigated the issue by enrolling and participating in VITA's Disaster Recovery Program. OSIG signed up for the program in 2020 and participated in 2021; OSIG has also begun preparing for the 2022 exercise.

Thank you for bringing this issue to our attention.

Sincerely,

A handwritten signature in black ink, appearing to read "Michael C. Westfall".

Michael C. Westfall, CPA
State Inspector General

November 15, 2021

TO: Staci Henshaw, Auditor of Public Accounts

FROM: Peter Blake, Director



RE: SCHEV response to the APA Information System Security Review for FY 2019

Develop and Implement Policies and Procedures

SCHEV acknowledges the APA's findings concerning our Policies and Procedures. As a small agency, we do have processes to meet Commonwealth security requirements, but we lacked formal guidance to provide evidence to auditors.

The SCHEV ISO is working with the agency head to adopt VITA's SEC501 Policy and Procedure templates to provide an agency-wide set of policies. The SCHEV ISO is also working with the System Administrators and our VITA ISO Liaison to create system manuals for each of our applications on Archer, which will cover the specific Information Security procedures necessary for each of our individual systems.

Improve Access Controls

SCHEV acknowledges the APA's findings concerning our Access controls. We are in the process of integrating a formal access removal process and checklist into our termination process so that we can verify removal of access to all SCHEV systems within 24 hours of departure, as required in Section PS-4 of the Security.

Improve Audit Logging Process

SCHEV acknowledges the APA's findings concerning our Audit Logging process.

We are working to with our VITA ISO Liaison to implement an audit logging and monitoring solution, subject to clarification on the rules and responsibilities of agencies using ECOS cloud services and VITA's own implementation of an LM application, currently in the testing process.

Update Contingency Plans and Perform Disaster Recovery Testing

SCHEV acknowledges the APA findings concerning our contingency plans and Disaster Recovery Testing.

As a small agency with all of our systems hosted by VITA or third party vendors, it is not easy for us to do an annual formal disaster recovery testing on all of our systems. We are working with

STATE COUNCIL OF HIGHER EDUCATION FOR VIRGINIA
101 N. 14TH STREET, RICHMOND, VA 23219

our VITA ISO liaison to review our COOP and BIA documents to create formal processes that will satisfy the requirements of CP-1-COV-1.

Improve Security Awareness Training

SCHEV acknowledges the APA findings concerning our Security Awareness Training. SCHEV conducts annual Security Awareness training, but we rely on the SANS Securing the Human modules provided by VITA. At the time of the audit, VITA was switching to a new software solution, which meant a few users were caught in the midst of training and unable to complete some modules.

The switchover to LITMOS has now been completed, and SCHEV has strengthened our formal onboarding process to ensure that every new hire is told of the need to complete security training and that the agency ISO is notified whenever there is a new hire. We anticipate that upon completion of the next round of annual training we will have 100% completion and will be able to maintain that rate going forward.

To: Auditor of Public Accounts

From: Executive Director Dr. Joe Keiper

Date: 19 January 2022

Re: APA Information System Security Review for FY2019

The results of the Audit have been reviewed. Due to COVID and staff turnover, there were several delays in getting a response to the Audit of Public Accounts. Numerous efforts have been underway since 2019 to create many of the instances pointed out in the report. We have a plan in place for moving forward and appreciate the assistance of the Audit of Public Accounts and their efforts to help the Museum understand areas where the systems can be improved.

We at the Virginia Museum are working toward providing a more secure IT infrastructure. The necessary steps are being taken to help ensure security in the future. Removal of legacy systems and increased distribution of information on current systems will help to increase security Museum wide. We will continue to be as vigilant as our ever-decreasing information technology budget allows.

Sincerely,



Dr. Joe Keiper
Executive Director
Virginia Museum Of Natural History



COMMONWEALTH OF VIRGINIA
Workers' Compensation Commission

333 E. Franklin St., Richmond, VA 23219
877-664-2566 | workcomp.virginia.gov

Robert A. Rapaport, Chairman
Wesley G. Marshall, Commissioner
R. Ferrell Newman, Commissioner
James J. Szablewicz, Chief Deputy Commissioner
Jason S. Quattropani, Clerk

Evelyn V. McGill
Executive Director

p. 804-205-3060
f. 804-823-6945

December 8, 2021

Ms. Staci Henshaw
Auditor of Public Accounts
101 North 14th Street, 8th floor
Richmond, VA 23219

Re: Virginia Workers' Compensation Commission FY2019 Audit Report

Dear Ms. Henshaw:

The Virginia Workers' Compensation Commission (Commission) appreciates your staff's efforts in reviewing the Commission's information technology operations for Fiscal Year 2019. The Commission is pleased with the findings which report full compliance with internal control requirements.

The Commission agrees with the Audit Report and findings. The Commission has worked hard to ensure that information security is a top priority and is pleased with the results shown in the report.

We look forward to a continued partnership with the Auditor of Public Accounts. Thank you for this opportunity to review and comment on the draft audit report.

Sincerely,

A handwritten signature in cursive script that reads "Evelyn V. McGill".

Evelyn McGill
Executive Director

RESPONSIBLE OFFICIALS

Department of Agriculture and Consumer Services

Bradley Copenhaver., Director

Department of Conservation and Recreation

Matthew Wells, Director

Department of Criminal Justice Services

Shannon Dion, Director

Department of Elections

Susan Beals, Director

Department of Forestry

Rob Farrell, State Forester

Department of Health Professions

David Brown, D.C., Director

Department of Housing and Community Development

Bryan Horn, Director

Department of Juvenile Justice

Valerie Boykin, Director

Department of Labor and Industry

Gary Pan, Director

Department of Military Affairs

Walt Mercer, Chief Operations Officer

Department of Energy

John Warren, Director

Department of Professional and Occupational Regulation

Demetrios Melis, Director

Department of Small Business and Supplier Diversity

Matthew James, Director

Indigent Defense Commission

David J. Johnson, Director

RESPONSIBLE OFFICIALS (continued)

Jamestown-Yorktown Foundation

Christy Coleman, Director

Office of the State Inspector General

Michael C. Westfall, State Inspector General

State Council of Higher Education for Virginia

Peter Blake, Director

Virginia Museum of Natural History

Joe Keiper, Director

Virginia Workers' Compensation Commission

Evelyn McGill, Director